TRUCOS WINDOWS: RECUPERAR DATOS BORRADOS POR ERROR



LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA



INTERNET
CÓMO FUNCIONA GOOGLE

LATEX
EDICIÓN DE TEXTOS PROFESIONAL AL ALCANCE DE CUALQUIERA

PROGRAMACIÓN
JOOMLA A TU MEDIDA

TECNOLOGÍA NAC
REDES SEGURAS Y MÁS CONTROLADAS



COMPARATIVA

Los antivirus a examen

Y ADEMÁS...
Cortafuegos de aplicaciones web

CURSO DE JAVA ÚTIL
jWadalPasswd (IV)

RETROINFORMÁTICA
Discos y memorias encriptadas



Directora: Montse Fernández
(montsef@mcediciones.com)

Colaboradores: Ferran Caldés, Toñi Herrero, Sara Rojas, Ana Rueda, Francisco Javier Palazón, Susana Velasco, Regina de Miguel, Laura Pajuelo, Jorge García López.

Fotógrafos: Sebastián Romero.

Maquetación: Domingo Melero.

Publicidad
Directora comercial: Carmen Ruiz
(carmen.ruiz@mcediciones.com)
Menchu de la Peña
(mdelapena@mcediciones.com),
Orense, 11. 28020 Madrid
Tel: 91 417 04 83 . Fax: 91 417 05 33

Suscripciones: Fernando García (fgarcia@mcediciones.com)
Tel: 91 417 04 83

Edita:



Editora: Susana Cadena
Gerente: Jordi Fuertes
Redacción, Administración y Departamento de Publicidad
Paseo San Gervasio, 16-20.
08022 Barcelona
Tel: 93 254 12 50 · Fax: 93 254 12 63

Oficina de Madrid
C/ Orense, 11 bajos
2820 Madrid
Tel. 91 417 04 83
Fax: 91 417 04 84

Distribución:
Coedis S.A. Avda. de Barcelona, 225 - Molins de Rei, Barcelona
Coedis Madrid: Alcorcón,9
Pol Ind. Las Fronteras-Torrejón de Ardoz, Madrid

Fotomecánica: MC Ediciones, S.A.
Paseo San Gervasio, 16-20.
08022 Barcelona

Impresión: Litografia Rosés

Tel. 93 633 37 37

Precio de este ejemplar: PVP 4,95 € (IVA incluido)
Precio para Canarias, Ceuta y Melilla:
4,95 € (incluye transporte)
Depósito legal: MA-1049-97 / nº146

LAS CLAVES DEL LIDERAZGO VIRTUAL Y DIGITAL HAN CAMBIADO

En el marco del ciclo de conferencias *Los debates abiertos de Fundación Telefónica*, el tecnólogo David Weinberger, coautor del influyente *The Cluetrain Manifesto: The End of Business as usual*, incidió en el hecho de que lo virtual ya es más real que la realidad en sí, en especial con la llegada de la web 2.0 y de las nuevas reglas que organizan el mundo de Internet.

David Weinberger, autor del libro *Everything is Miscellaneous. The Power of the New Digital Disorder*, es sin duda uno de los primeros que tuvieron la visión de las nuevas reglas que iban a regir la llamada web 2.0, en la que ya estamos inmersos. Para Weinberger, "las empresas que no controlan ciertos negocios deciden hoy en día agruparse, con esa mentalidad colaboradora, con aquellas que saben", debido en gran parte al cambio de concepción de las estrategias de liderazgo. "Ahora asistimos a un nuevo modelo de liderazgo, el distribuido, basado en una especie de meritocracia y mucho más complejo".

Hay, en definitiva, un nuevo orden, en el que las claves del liderazgo virtual y digital de las grandes empresas ha cambiado. Por otro lado, según el experto norteamericano "las conversaciones de mercado en la Red tienden a ser bastante objetivas, con Internet, el comercio se modifica y se mejora".

Para Weinberger los hipervínculos de la Red son ya un medio colectivo en un mundo en que la riqueza y la abundancia de la información han proporcionado a las empresas nuevas categorías de trabajo de carácter ilimitado. Además, señala que se hace urgente una reflexión sobre cómo estos cambios que han venido de la mano de la web semántica han afectado no sólo a los negocios, sino también a la educación y a la política.

[SUMARIO número 146]

3. Editorial
4. Noticias
10. Hack: Conficker
16. Crack: Cortafuegos
22. Hack: Seguridad
28. Hack: Tu blog. Cómo funcina Google
32. Curso de Java Útil: jWadalPasswd (IV)
38. Programación: Joomla a tu medida
46. Programación: Observer
51. Algarroba
66. Tecnología: DNI Electronico
72. Hack: Tecnología NAC
76. Zona de juegos:
- Fifa 10
- Naruto Shippuden
- Ninja Council 3
- Marvel: Ultimate Alliance 2
80. Trucos:
- Pandora Recovery
- Troyanos
- Antivirus
82. Zona de juegos móviles:
- Looney Tunes Monster Match
- Mini Golf Chihuaca
- World Series of Poker Pro Challenge



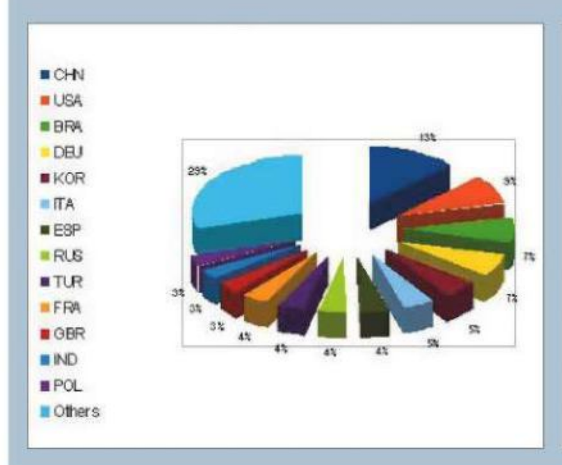
La infección de un PC zombie puede durar más de dos años

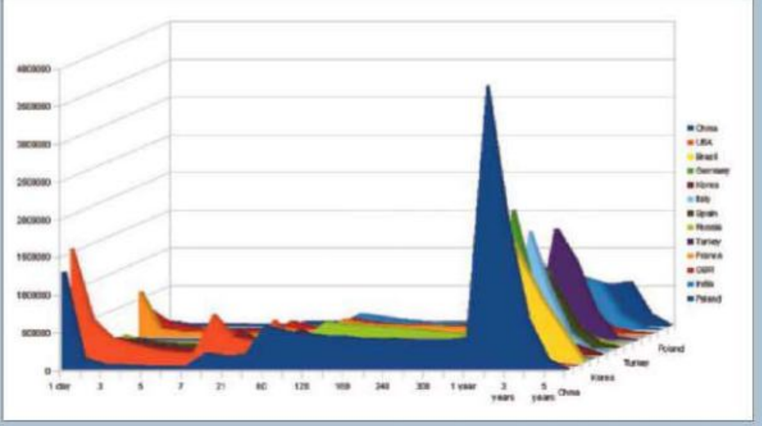
En un primer momento, los expertos de la industria estimaron que el tiempo medio que un equipo informático permanecía infectado era de seis semanas. Sin embargo, un reciente informe de Trend Micro pone de manifiesto que esta estimación está lejos de ser exacta.

Así, durante el análisis de más de 100 millones de direcciones IP comprometidas Trend Micro ha identificado que el pico de IPs infectadas -direcciones que pertenecen a botnets o redes zombie- (o que son infectadas repetidamente) permanecen en este estado durante más de 2 años, aunque la media de infección es de 300 días en los principales países.

El término botnet o red zombie se utiliza para designar a los ordenadores que forman parte de una red robot tras haber sido infectados por algún tipo de malware. Estos equipos pueden ser controlados por terceras personas con fines ilícitos (distribuir spam, robo de identidad, robo de información confidencial,...) sin que el usuario sea consciente de ello. Según las estadísticas de Trend Micro, el 80% de todos los equipos comprometidos han estado infectados durante más de un mes.

Una vez que el equipo pasa a estar comprometido, no es raro encontrar que se ha convertido en parte de una botnet más amplia. Las redes zombies con frecuencia causan daño en la forma de los ataques de malware, fraude, robo de información y otros crímenes. En lo que va de 2009, casi todo el malware rastreado por los expertos de Trend Micro está siendo utilizado por los cibercriminales para robar información (credenciales, etc.) principalmente. Hasta ahora, las tres redes zombie que son más peligrosas en relación con el robo de identidad, información financiera y de cualquier otro tipo son Koobface, ZeuS/Zbot e Ilomo/Clampi.





Versión gratuita de su suite de seguridad empresarial

En su nueva versión 4.1, FortiClient ofrece nuevas funcionalidades que incluyen SSL VPN, optimización WAN, detección de aplicaciones y control endpoint, mientras que proporciona una infraestructura para el cumplimiento de las políticas de seguridad totalmente gestionable, para ayudar a las empresas a reducir su exposición a las amenazas de ciberseguridad. Con FortiClient 4.1 se dota de protección completa para portátiles y PCs y puede ser implementada modularmente para coexistir con otros productos de seguridad dedicados al endpoint. Fortinet también ofrece una versión de FortiClient 4.1 estándar y gratuita para los consumidores y pequeñas y grandes empresas que buscan una protección completa para sus portátiles y ordenadores personales. Mientras que muchas soluciones de seguridad en el endpoint disponibles en el mercado sólo proporcionan protección firewall y/o antivirus, tanto la versión gratuita como la licenciable de FortiClient 4.1 ofrecen el enfoque de consolidación con funcionalidades propias de los dispositivos de Fortinet para la seguridad de red en entornos corporativos FortiGate. Ambas versiones también reciben actualizaciones automáticas de los servicios de suscripción FortiGuard para asegurar la protección frente a las nuevas amenazas.





Expertos en seguridad para analizar amenazas cibernéticas

Symantec anuncia su programa Cyber Threat Analysis Program (CTAP), un enfoque completo que captura e identifica de forma global los datos pertinentes en materia de seguridad, proporciona la identificación de amenazas localizadas, ofrece las soluciones y medidas adecuadas para proteger la información crítica del cliente y mejorar de forma generalizada su seguridad. CTAP proporciona acceso a uno de los repositorios comerciales más grandes de seguridad cibernética centrado en amenazas y datos vulnerables, y también al conjunto de herramientas de seguridad más amplio de Symantec. La compañía ofrece este acceso a través de analistas expertos *in situ* con el fin de fortalecer la posición de defensa de la empresa y aumentar su capacidad proactiva. Además de los servicios integrados de inteligencia de seguridad de Symantec, CTAP está diseñado para ampliar la visión del cliente en lo que respecta el terreno de amenazas, y proporcionar recursos para mitigar los riesgos de forma efectiva y responder a necesidades específicas según se requieran. El programa hace uso de la extensa Red Global de Inteligencia de Symantec y de su amplio y exclusivo conocimiento sobre seguridad con el fin de proporcionar a los clientes informes detallados sobre los ataques, actividad de código malicioso, phishing y spam que experimenta la empresa a diario. El volumen XIV del Informe de amenazas de seguridad de Internet de Symantec, publicado en abril de 2009, demostró el alcance al que llegan las amenazas de seguridad cibernéticas de hoy en día. Symantec creó más de 1,6 millones de firmas de código malicioso en 2008 y bloqueó una media de más de 245 millones de intentos de ataques de código malicioso al mes en todo el mundo durante 2008. Además, el 90 % de todas las amenazas detectadas por Symantec durante el período del estudio pretendían robar información confidencial. Como parte de CTAP, el programa fusiona los datos del cliente y los datos públicos con la inteligencia CTAP con el fin de identificar de forma rápida las amenazas de seguridad cibernéticas, determinar la verdadera naturaleza de los ataques, desarrollar contramedidas e implementar soluciones.

Nueva solución de conectividad móvil 3G



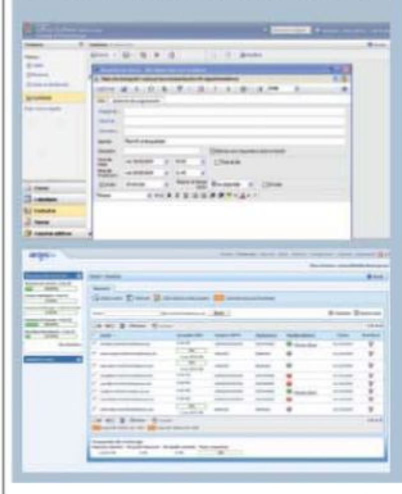
Este nuevo dispositivo modular, denominado WatchGuard 3G Extend USB, complementa y amplía las capacidades de su reconocida familia de appliances de seguridad de red para la gestión unificada de amenazas (UTM).

El nuevo dispositivo está diseñado para aquellos negocios que necesitan conectividad de alta velocidad para redes de comunicación extendida (WAN), en los que el ancho de banda del cableado directo es demasiado caro o simplemente no está disponible. Por ejemplo: oficinas temporales o remotas así como centros de venta al minorista, quioscos, cajeros automáticos y otros recursos móviles tales como vehículos de policía, trenes o camiones que realizan largos recorridos. Con este dispositivo, las empresas ganan en seguridad y obtienen un acceso a Internet de alta velocidad que puede ser utilizado para una conexión de red principal, en caso de fallo de la WAN o de sobrecarga del 3G wireless.

WatchGuard 3G Extend USB actúa como un puente inalámbrico L2TP 3G (componente hardware para conectar dos o más segmentos de la red) y lleva la conectividad a Internet a los appliances de seguridad de red UTM de WatchGuard. Dado que soporta módems de telefonía móvil de alrededor de 2.000 ISPs, los clientes de todo el mundo pueden elegir entre un amplio abanico de proveedores de servicios móviles dependiendo del que mejor les venga en función su ubicación, de los requerimientos de servicio o de las necesidades presupuestarias. El diseño modular del WatchGuard 3G Extend USB también proporciona a las empresas una gran flexibilidad y escalabilidad ante el despliegue de proyectos. Por ejemplo, el dispositivo puede ser fácilmente trasladado o transferido entre otros appliances WatchGuard ofreciendo a las compañías, de este modo, un modelo con un excelente TCO y protegiendo su inversión frente a futuras actualizaciones.

Arsys.es combina Exchange con el correo electrónico convencional

Hasta ahora, el correo electrónico corporativo tenía que optar entre las prestaciones de Exchange o las tradicionales y económicas cuentas POP/IMAP ya que ambos sistemas no resultaban compatibles en un mismo dominio. Esta incompatibilidad incrementaba los costes en comunicaciones de muchas empresas, que se veían obligadas a adoptar Exchange para todas las cuentas de su correo corporativo o tenían que buscar un dominio secundario, con la consiguiente confusión entre los usuarios. Sin embargo, la plataforma Correo Híbrido de arsys.es permite que estas tecnologías estén operativas bajo un mismo dominio, según las necesidades de cada empresa. Este sistema permite, incluso, pasar una cuenta puntualmente de POP/IMAP a Exchange y viceversa, dependiendo de la movilidad de los empleados. De este modo, cualquier persona puede gestionar eficientemente sus recursos profesionales en todo momento, aprovechando las herramientas de productividad de Exchange y accediendo a los datos corporativos, independientemente de su lugar y dispositivo de acceso. Para Fermín Palacios, Director de Negocio de arsys.es, “en la mayoría de las empresas hay usuarios móviles, que viajan y necesitan consultar su correo electrónico o su agenda constantemente, y otros usuarios que permanecen en la oficina durante su jornada. Esta plataforma permite que cualquier persona incremente su productividad profesional fácilmente y con el máximo control de la inversión en todo momento”.





El mercado negro de Internet, una economía sumergida donde todo tiene un precio

Los datos robados de una tarjeta de crédito tienen un precio de mercado de unos 300 euros. Un ataque DDoS (Distributed Denial of Service), un ataque que satura e inutiliza los servidores de las víctimas) de una hora de duración puede costar unos 150 euros. Y se pagan hasta 800 euros por un millón de correos spam. Estas y otras cifras salen a la luz gracias a las últimas investigaciones de los laboratorios de seguridad de G Data Software centradas en la industria del cibercrimen.

El equipo de G Data Software se camufló en los sórdidos círculos de acción de hackers, ladrones de datos y demás delincuentes digitales durante los meses de junio y julio de este año y descubrieron que el escenario se ha profesionalizado al máximo dando lugar a una economía perfectamente organizada. Al frente de la organización existen proveedores que ofrecen 'hosting a prueba de balas' que permiten la existencia de foros y tiendas online ilegales en las que los ciberdelincuentes ofrecen sus servicios y se ponen en contacto con los posibles compradores. Los foros ilegales son el centro neurálgico de este ámbito. Allí quienes se inician en estos bajos fondos digitales se encuentran con sus mentores que, tras cobrar una considerable cantidad de dinero, les enseñan todos los secretos del negocio. Aquí también contactan los vendedores y compradores de este mercado negro. Y en las salas privadas de estos foros, de acceso exclusivo para cibercriminales bien conocidos y de prestigio, se intercambian todo tipo de productos y servicios. Los principales acuerdos suelen hacerse fuera de los foros, a menudo a través de ICQ o canales IRC manipulados (dos sistemas de mensajería instantánea).

Además, cualquiera que prefiera hacer negocios en un entorno todavía más profesional puede recurrir a una de las muchas tiendas online ilegales que existen. Aquí, los compradores pueden beneficiarse de importantes descuentos al adquirir grandes cantidades de datos robados, e incluso se les devuelve el dinero si no quedan satisfechos con el servicio. De tal forma, si los datos de tarjetas de crédito recién adquiridos no fuesen válidos ya -al haber cancelado el usuario legítimo dicha tarjeta-, se pueden reclamar otros datos o la devolución del dinero.

Junto a los datos robados, existen otros servicios también muy populares. Los principiantes suelen solicitar ataques DDoS. Para mantenerse al frente de esta competición, algunos actores de este mercado ofrecen este servicio por la pequeña cantidad de 10 euros por hora de ataque o 50 euros por día. Pero un buen precio no es la única herramienta de marketing a la que recurren los cibercriminales: incluso contratan banners publicitarios para anunciar sus servicios.





Distribución masiva del virus Induc a través de un e-mail que usa una citación judicial como gancho

Más de 3.500 usuarios con ordenadores infectados con el virus Induc ha detectado ya PandaLabs. Igualmente, se está viendo una alta actividad de distribución de este virus que llega a los usuarios a través de un correo electrónico remitido por la Guardia Civil, en concreto figura como remitente delitos.tecnologicos@policia.es y con el asunto 'Convocatoria en la Audiencia'. Dicho mensaje lleva adjunto un archivo que parece un pdf, -'Convocatoria10-pdf'- pero que realmente tiene la extensión .scr. Este archivo supuestamente contiene la convocatoria en sí misma. Al abrirlo, se descarga e instala el virus Induc.

Este virus fue detectado por primera vez el pasado mes de agosto y hasta la fecha, se distribuía solamente por transferencia de archivos a través de FTP, canales de IRC, redes P2P, USB's, etc. "Hasta ahora nunca se había distribuido por correo electrónico ni había utilizado técnicas de ingeniería social para hacer picar a los usuarios e incitarles a abrir el fichero adjunto", comenta Luis Corrons, Director Técnico de PandaLabs. El Ministerio del Interior ha alertado a los usuarios y se han colgado recomendaciones en las webs de las autoridades nacionales entre las que figura la más obvia: no abrirlo.



McAfee Family Protection, para la tranquilidad de los padres

McAfee ha anunciado el lanzamiento de McAfee Family Protection, un nuevo programa informático que protege a los niños de los peligros de la red, tales como la visualización de contenido inapropiado, verse involucrado en ciberacoso o la realización de interacciones arriesgadas en las redes sociales. McAfee Family Protection permite a los padres monitorizar y rastrear las actividades online que llevan a cabo sus hijos, y utilizar estos datos para enseñarles hábitos seguros y responsables en Internet. "Las ciberamenazas están aumentando exponencialmente, al mismo tiempo que cada vez más niños pasan su tiempo de ocio en la red. Vemos estos peligros cada día y son realmente una amenaza para los más pequeños" afirma Alfredo Vázquez, Director de Retail para EMEA y padre. "Son necesarias tanto la educación como la tecnología para proteger a nuestros hijos de los peligros de Internet, y McAfee Family Protection es la herramienta ideal para que los padres puedan mantener a sus hijos a salvo, de forma sencilla, cuando navegan por Internet". Recientes estadísticas muestran que el 62% de los padres se preocupan tanto o más por la seguridad de sus hijos cuando navegan por Internet que por lo que hacen cuando salen con sus amigos los fines de semana. Además el 52% de los adolescentes reconoce haber revelado información personal a desconocidos través de la red. Y uno de cada 17 niños ha sido acosado, amenazado o intimidado a través de la red. Con McAfee Family Protection, los padres pueden recibir alertas por correo electrónico y SMS cuando alguno de sus hijos ha accedido a un sitio web prohibido; pueden filtrar videos inadecuados en YouTube, y pueden bloquear programas de mensajería instantánea o correo electrónico peer-to-peer o sitios web con funciones parecidas. Los padres que trabajan o viajan y no tienen acceso físico al ordenador familiar pueden ajustar la configuración del programa de forma remota simplemente accediendo a www.mcafeefamilyprotection.com y accediendo a su cuenta personal.





Alerta: Los spammers se adelantan a la Navidad

Este año los ciberladrones se han adelantado a las fechas navideñas para reinventar nuevos ataques informáticos y pillar desprevenidos a los usuarios. Los spammers saben que la Navidad es una de las épocas del año donde se consume más: regalos navideños, compras espontáneas o viajes, mediante la compra online. Es aquí cuando entra en juego la astucia del pirata para aprovecharse del momento y de la buena voluntad de los usuarios para empezar a crear nuevas oleadas de ataques informáticos antes de la llegada de la Navidad. Por ello SPAMfighter avisa a todos los usuarios que tengan cuidado al abrir y leer e-mail, o al adquirir productos a través de correos de dudosa procedencia. SPAMfighter ha detectado que durante esta Navidad aumentará considerablemente el envío de spam. Los ataques son cada vez más sofisticados y con contenidos dedicados a distintos países. Martin Thorborg, cofundador de SPAMfighter, señala que "se trata de la primera ola de correo basura que se empieza a detectar y que a medida que nos acerquemos a las fiestas navideñas irán aumentando considerablemente". SPAMfighter realiza una serie de recomendaciones básicas que no está de más tener presente para transmitir a quiénes les pueda hacer falta. A saber: no hacer compras online a través de un correo electrónico de dudosa procedencia, aunque se trate de una excelente oferta; la caridad, antes y durante las fechas navideñas, es una de las técnicas más utilizadas por los ciber-delincuentes para estafar. Si se hacen donaciones es mejor conectarse a la web de la organización en cuestión; crear una cuenta de correo gratuita para las compras online y así evitar posibles amenazas. Realizar un seguimiento de dichas compras online; y antes de hacerlas, descargar o actualizar el filtro anti-spam para estar protegido.

Llaves USB JetFlash de Transcend

Transcend anuncia que sus llaves USB JetFlash han superado los test de compatibilidad con Windows 7 y están totalmente cualificados para incorporar el logo 'Compatible con Windows 7'. Las series V, las series T y las series Hi-Speed de las llaves USB JetFlash de Transcend han sido preparadas para superar los estrictos estándares de Windows 7, lo que asegura una completa funcionalidad cuando se utiliza este nuevo sistema operativo. Los usuarios pueden ahora usar tranquilamente las llaves USB de Transcend en ordenadores con sistema operativo Windows 7 sin preocuparse por la compatibilidad.

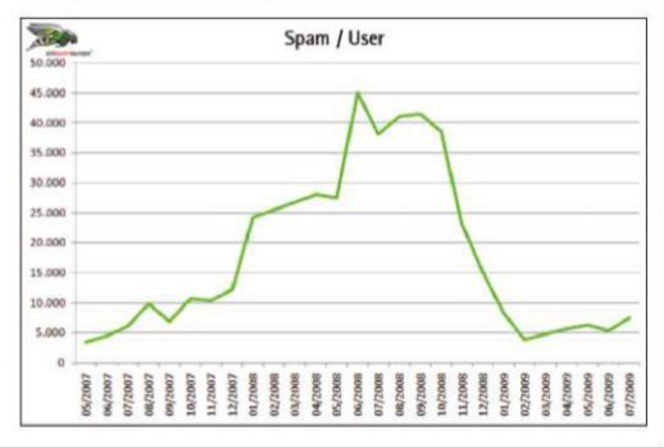


Menos spam pero más sofisticado

Según el informe semestral de la evolución del correo basura de Antispameurope, de enero a junio de 2009, los niveles de spam han sufrido una intensa caída que se inició a finales de 2008. Sin embargo, a pesar de esta bajada, se está detectando una profesionalización del spam, con un tipo de correos maliciosos de más difícil detección

La primera mitad de 2009 ha supuesto un respiro en lo que al número de spam se refiere. Así lo refleja el informe semestral elaborado por Antispameurope, empresa especializada en la gestión de la seguridad del correo electrónico. A finales del año 2008, ya se empezó a registrar una tendencia bajista del número de "correos basura" recibidos por cada usuario. Así, el año cerró con una media de 12.500 correos de spam recibidos al mes por cada usuario. Cifra que no tenía ya nada que ver con los niveles detectados, por ejemplo, en octubre, en los que el número ascendía a 38.500. El número registrado en diciembre, descendía aún más al comenzar 2009, mes en el que cada usuario recibió unos 8.000 mails basura al mes. El spam siguió bajando a lo largo del mes de enero hasta alcanzar los 4.500 correos de spam recibidos en febrero, cifra que será la más baja registrada en la primera mitad de 2009. Del mes de febrero a mayo se observa una tendencia alcista del spam. Siendo mayo el punto más alto con unos 6.500 correos no deseados recibidos al mes por cada usuario. A pesar de ser el punto más alto alcanzado en la primera mitad de 2009, dicho número no puede equipararse al alcanzado en junio del año anterior, mes en el que se llegaron a recibir 45.000 correos basura al mes. Sin embargo, en junio de este año el correo no deseado sólo llegaba a los 5.000 mails por usuario. A pesar de esto, hay que tener en cuenta que a partir de junio se observa una subida de los niveles de spam. Dicha tendencia alcista, se mantendrá hasta finales de año, aunque no se alcanzarán unos niveles muy altos.

Una de las principales conclusiones que se apunta desde el informe de Antispameurope es que, puede que el número de spam se reduzca en número pero no así en su sofisticación. Es decir, los spammers han creado nuevos mensajes de correo no deseado cuyo formato hace más difícil la detección. Gracias a la gran cantidad de información disponible en Internet, contando con las redes sociales, los creadores de spam disponen de los datos suficientes para dirigir mejor sus correos y hacer que sea más personalizado y efectivo. Por ejemplo, una vía que utilizan mucho los spammers es la detección de las compras online que se puedan realizar, de tal manera que pueden saber cuáles son los gustos del usuario y enviarle así un mensaje que llame más su atención. Debido a esta personalización del spam será más difícil de detectar por el usuario y, por tanto, más peligroso. En resumen, al spammer no le interesa tanto enviar una gran cantidad de mensajes sin resultado alguno, sino enviar mensajes efectivos con los que puedan obtener resultados.



Conficker: el gusano del 2009

Las amenazas que se propagan a través de Internet crecen año a año. Durante el 2009 el ataque más temido ha sido el del gusano Conficker. La psicosis que desató durante sus primeros meses de existencia ha parado, pero sus ataques no han desaparecido.

Las amenazas que se propagan a través de Internet crecen año a año. Durante el 2009 el ataque más temido ha sido el del gusano Conficker. La psicosis que desató durante sus primeros meses de existencia ha parado, pero sus ataques no han desaparecido.

Internet es un lugar cada vez más inseguro. El número de programas, documentos y mensajes que tratan de infiltrarse en los equipos para utilizar los recursos del sistema infectado (conocidos como malware) es innumerable y las amenazas se multiplican cada día, apareciendo por centenares.

Además, las ya conocidas también van variando para intentar conseguir un mayor grado de incidencia en la Red. Uno de los ataques más temidos es el de los gusanos, que se alojan en la memoria del equipo y se duplican a sí mismos con el objetivo crear una cadena de contagios. Como utilizan partes del sistema operativo invisibles al usuario, éste no se da cuenta de su presencia hasta que su red comienza a ralentizarse tanto que los programas más básicos tardan mucho en arrancar. Incluso pueden llegar a controlar el ordenador por completo.

La característica más determinante de este tipo de ataques es la velocidad con la que se propagan de un equipo a otro. Tanto es así que desde que es localizado por primera vez por un centro de seguridad hasta que se extiende por equipos de todo el mundo pasa muy poco tiempo. Es precisamente lo que pasó con Conficker, el gusano más peligroso de los últimos años. Este "bichito" ha mantenido alerta a la comunidad virtual durante muchos meses, y cuando parecía que había desaparecido, de nuevo encabeza las listas de contagios mundiales.

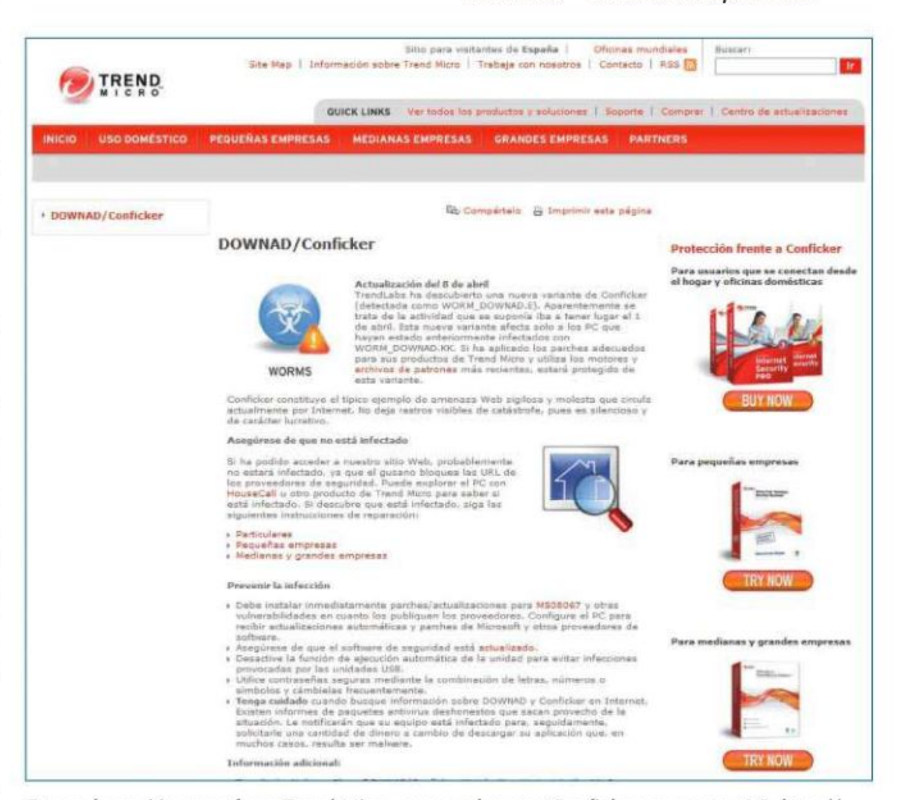
El gusano rebelde

Con las pretensiones actuales de los ciberdelincuentes parecía difícil que un ataque a otros equipos. Así se multiplica fácilmente y contagia al máximo número de ordenadores posible.

Una vez dentro de un ordenador cualquiera, el gusano desencadena una serie de procesos que reducen la seguridad del sistema sin que el usuario se de cuenta de nada. Por ejemplo, desactiva las actualizaciones automáticas de Windows: Windows Security Center, Windows Defender y Windows Error Reporting. Además, como no permite que el equipo esté al día impide la descarga del parche que puso Microsoft a disposición de todos los clientes Windows en octubre de 2008. De hecho, va un paso más allá, y es que también lo bloquea (para todos aquellos que lo descarguen directamente), de tal manera que si se instala después del contagio, no es efectivo.



En la captura de pantalla del cuadro de diálogo de reproducción automática, el gusano agregó la opción Abrir la carpeta para ver los archivos — Proveedor no especificado. La opción resaltada — Abrir la carpeta para ver los archivos — usar el Explorador de Windows es la opción proporcionada por Windows y la que debería usar. Si selecciona la primera opción, el gusano se ejecuta y puede comenzar a extenderse a otros equipos. El gusano agregó la opción Abrir la carpeta para ver los archivos — Proveedor no especificado.



Esta es la opción que ofrece Trend Micro para acabar con Conficker en nuestro PC: http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/SysClean-WORM_DOWNAD.zip

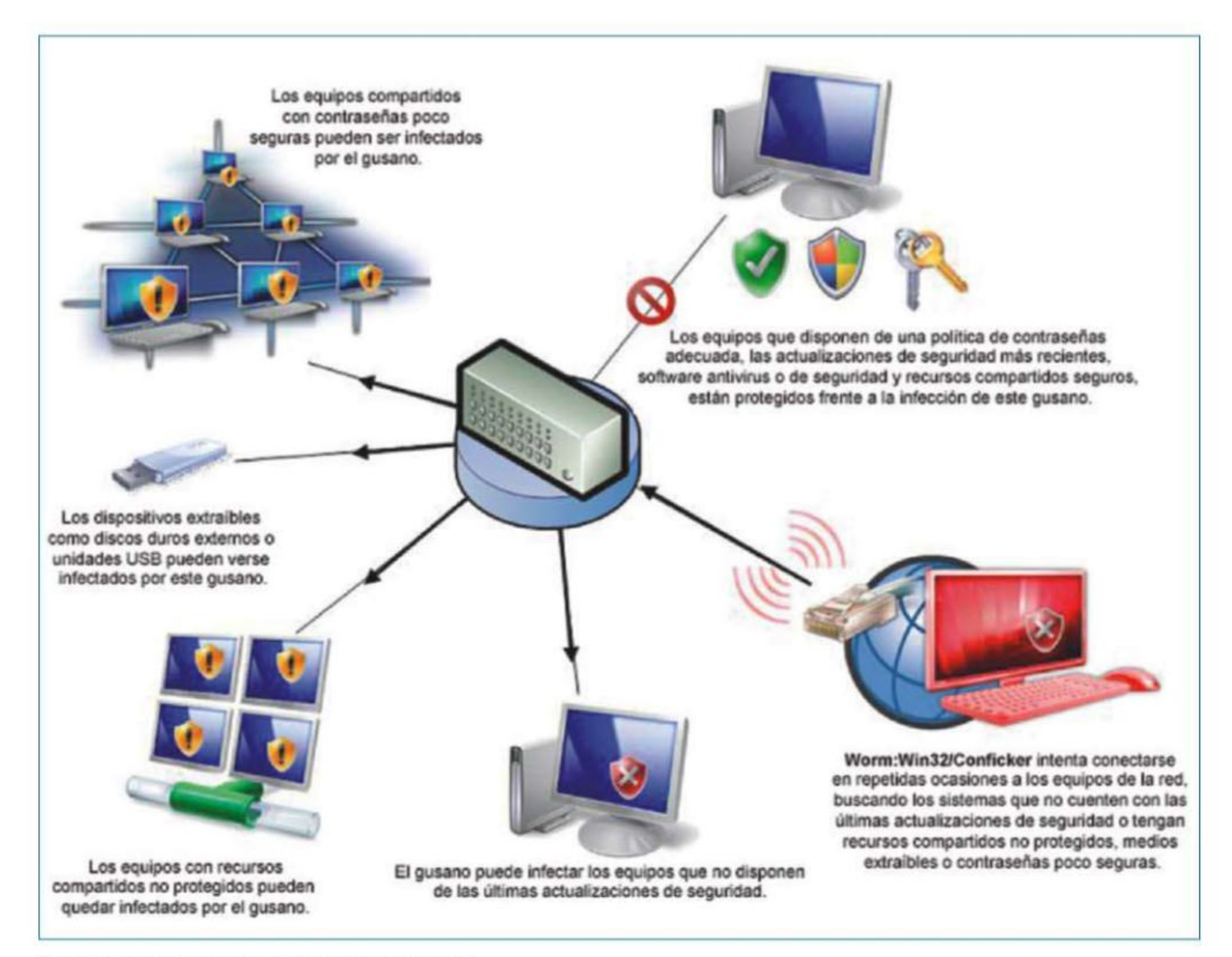
>>> CÓMO EVITAR UN CONTAGIO

- **Lo esencial para impedir que Conficker entre en el equipo es mantener el sistema operativo actualizado. A partir de ahí, se pueden emprender algunas acciones muy sencillas que evitarán que ésta y otras amenazas malware encuentren vía libre hacia nuestro ordenador.**
- **Deshabilitar la función de reproducción automática, que permite que se ejecute un programa o acción al insertar un CD/DVD o cuando se conecta un dispositivo de almacenamiento externo como un USB. Para quitarlo hay que acceder al registro del sistema (escribiendo "regedit" en la opción ejecutar) y modificar el valor de algunos registros.**
- **Buscar contraseñas "fuertes" para los recursos compartidos en red. Las más seguras son las largas, que combinan mayúsculas y minúsculas, y también letras y números.**
- **Proteger el ordenador con una solución de seguridad compuesta por un firewall, antivirus y otras herramientas. Además, debe estar siempre actualizado.**

que de malware se dirigiera a conseguir un contagio masivo, ya que la tendencia es olvidarse de la fama y buscar el beneficio económico. Para ello, es sin duda más eficaz un ataque centralizado. Aun así, y al más puro estilo de Blaster, que trajo bastantes quebraderos de cabeza hace algunos años, el gusano de nombre Conficker (aunque también se le conoce como Downadup) demostró que no era así.

Allá por noviembre del pasado año, todos los centros de detección de amenazas de las distintas firmas de antivirus dieron la alarma: un nuevo gusano estaba infectando ordenadores por todo el mundo a una velocidad completamente inesperada. En enero, solo tres meses después, los usuarios afectados por Conficker se contaban por millones. Este gusano, todavía activo, aprovecha una vulnerabilidad (MS 08-067) en el servicio de servidor de Windows para introducirse en los ordenadores.

Su modus operandi es muy sencillo: lanza una petición masiva y envía un archivo malicioso a los equipos vulnerables, en los que instala un servidor http que, a su vez, envía mensajes de comprobación



Esquema del funcionamiento de Conficker en el ordenador.

Durante meses su objetivo no ha estado nada claro. En general, se puede decir que crea una red de tipo botnet con todos los ordenadores infectados para llevar a cabo actividades como el envío de spam a otros equipos. Estos mensajes no deseados consiguen saltarse los filtros antispam porque utilizan un dominio único en el vínculo que incluyen. A parte de esa función, sus actividades se desarrollan en otro sentido: el scareware. Este término se utiliza para denominar los programas de software antimalware falsos que circulan por Internet. En este caso, Conficker descarga algunos programas a los equipos infectados como el Adware/AntiVirus2009 o el Spyaware Protect, que generan avisos falsos de infecciones en el sistema. Al principio inundan a los usuarios con este tipo de alertas, pero luego pasan a anuncios para que compren el software, que mantendrá sus equipos a salvo. Cuando lo hacen, pagan unos 50 dólares por programa que, en realidad, no sirven para nada. Esta es, de hecho, una de las principales amenazas a las que se enfrentan los internautas hoy en día según Microsoft.

También por USB

Si el contagio a través de Internet fuera la única opción para Conficker, el parche y un antivirus actualizado lo habrían neutralizado y probablemente a estas alturas ya estaría olvidado. Pero aunque es cierto que normalmente llega por correo

>>> ALGUNOS IMITADORES

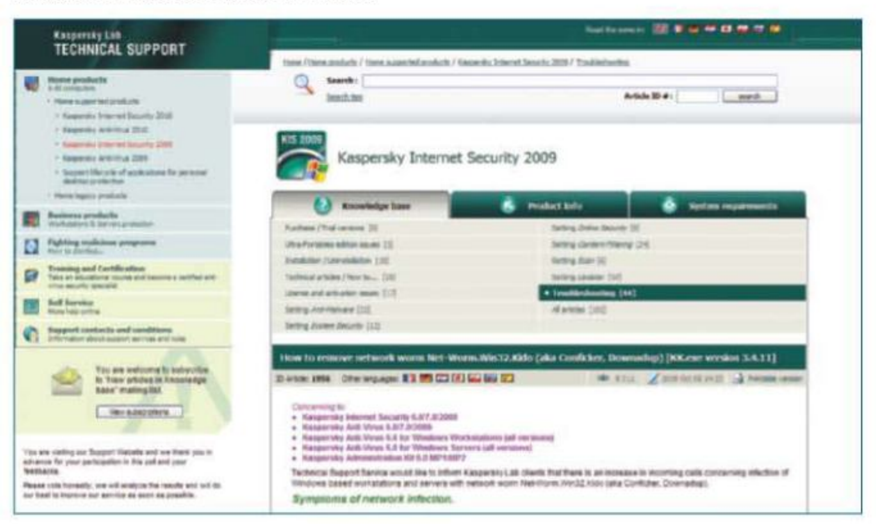
El gusano Conficker, además de infectar millones de ordenadores por todo el mundo, está sirviendo como un modelo para otras amenazas malware, sobre todo por su notoriedad. Un claro ejemplo es el renacimiento de un virus que surgió en 2005, Neeris. Cuando apareció era un programa que actuaba a través de IRC (sitios de chat en línea) y se expandía principalmente a través de enlaces en el programa de mensajería instantánea MSN Messenger. Con su nueva versión ha adoptado algunas de las estrategias de infección de Conficker. Entre ellas, ataca la misma vulnerabilidad, se reproduce a través de unidades flash, de la función Autorun y servidores SQL. La parte positiva es que se elimina exactamente igual debido a su similitud.



Herramienta de Bitdefender que elimina este programa malicioso: http://www.bdtools.net/



Sophos cuenta con esta herramienta para exterminar Conficker de nuestro ordenador: http://www.sophos.com/kb/54457.html



Por su parte, Kaspersky nos permite eliminar Conficker con esta herramienta: http://support.kaspersky.com/faq/?qid=208279973

electrónico, desde redes de descarga de archivos o a través de páginas maliciosas, ha encontrado otra manera de pasar de un equipo a otro: oculto en los dispositivos de almacenamiento. Escondido en una memoria USB, disco duro externo y hasta tarjetas de memoria, accede al equipo desde uno de sus puertos y ni el firewall ni el antivirus pueden hacer nada (a menos que se sea uno de los pocos usuarios que revisa los dispositivos antes de abrirlos, por supuesto).

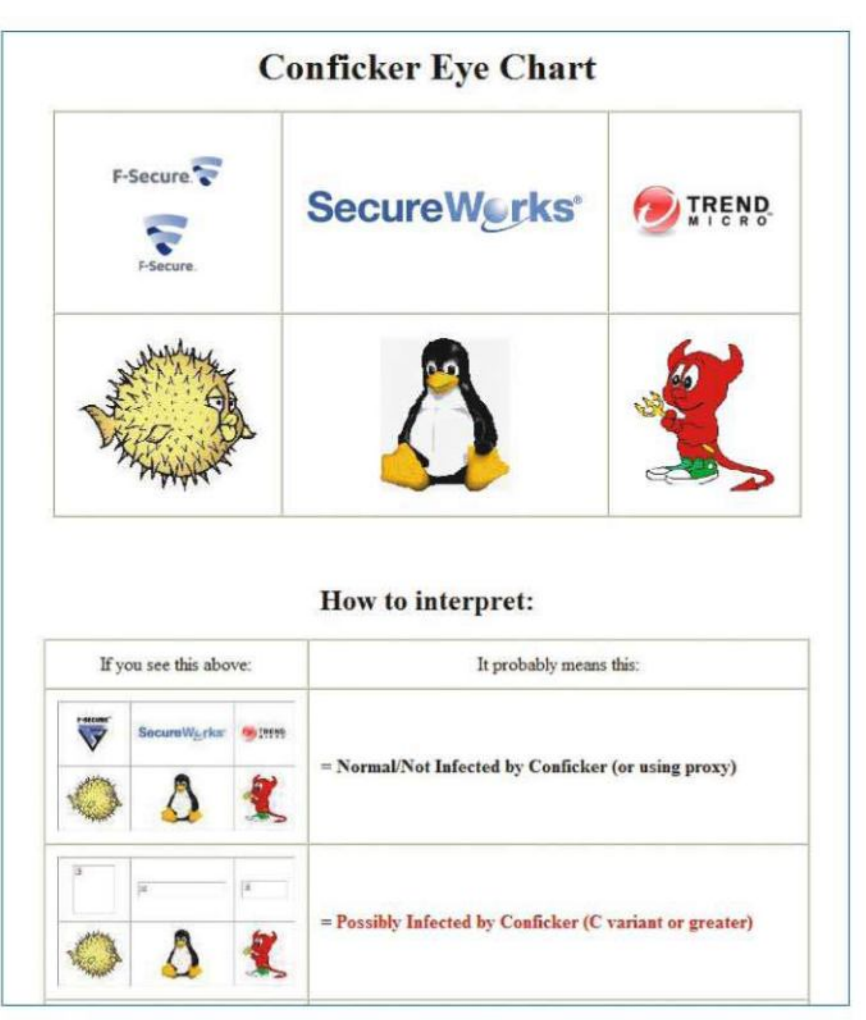
Su actuación es, de nuevo, muy sencilla. En la mayoría de los casos, los ordenadores tienen activada la función de reproducción automática (Autorun), que viene predeterminada. Con ella, cada vez que se introduce uno de estos soportes en el ordenador, el sistema lo lee automáticamente y aparece la conocida ventana de opciones.

Conficker convierte la de "abrir la carpeta" en un documento ejecutable. Cuando un usuario pulsa sobre esta opción pensando que va a ver lo que hay dentro de, por ejemplo, una memoria USB, lo que realmente está haciendo es poner en marcha el gusano, que pasa a instalarse en su ordenador. Otra de las formas de contagio que ha encontrado es propagarse es a través de los documentos compartidos en una red, porque es capaz de descifrar las contraseñas débiles y así pasar de un equipo a otro.

Conficker tiene cura

Para llegar a esta versatilidad el gusano ha tenido que evolucionar, y ha tenido un año entero para ello. Hasta el día de hoy se conocen distintas versiones, cada una de ellas identificadas con una letra al final de nombre del gusano (por ejemplo, Conficker.A o Conficker.B).

La última de ellas, Conficker.E, fue denunciada por Microsoft en el mes de abril. A partir de ese momento, el número de contagios empezó a decaer considerablemente, aunque en las últimas semanas se ha vuelto a alertar de su fuerte presencia. Un claro ejemplo es el caso del informe mundial de detección de amenazas elaborado por ESET, que ha constatado que durante el mes de agosto el gusano encabezaba la lista de malware más difundido, con algo más del 8,5% de las infecciones a nivel global.



Debido a que Conficker bloquea el acceso a gran cantidad de páginas de seguridad, es posible que tenga problemas para actualizar su antivirus y probar antivirus en línea, en este caso el Conficker Working Group ha creado un sencillo test de visualización de imágenes, puede accede a él desde este enlace, en el que también se indica cómo interpretar el resultado de las imágenes vistas: http://www.confickerworkinggroup.org/infection_test/cfeyechart.html



Esta es la opción de ESET para eliminar el gusano: http://www.eset-la.com/support/tools.php

>>> EL DÍA DE LOS INOCENTES

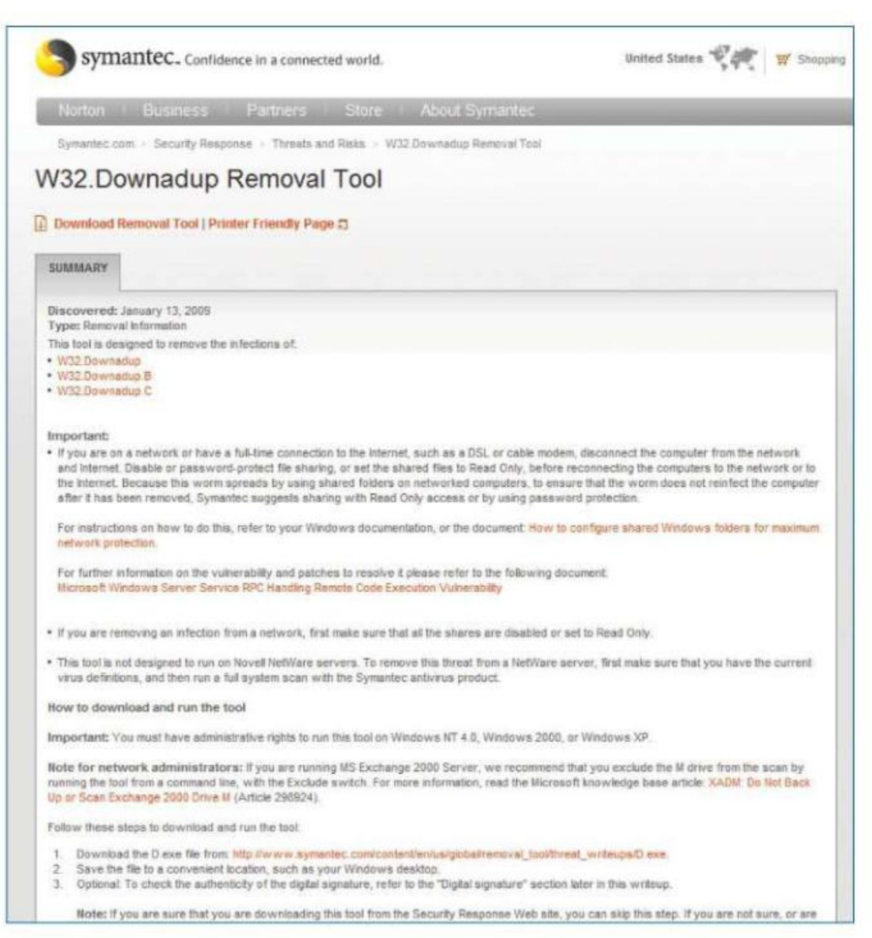
El 1 de abril se celebra en los países anglosajones el día de los inocentes, y en este 2009 todo el mundo estaba pendiente de Conficker. La alarma se extendió desde varias empresas de seguridad informática, que temían que la tercera reencarnación del virus, Conficker.C, se activara e infectara miles de ordenadores. Broma o realidad, lo cierto es que el gusano, aunque con nuevas mejoras, siguió el curso que estaba tomando hasta el momento.

El dato en España es aún más importante, ya que la cifra aumenta hasta el 9,55% del total de las detecciones durante el mismo mes. Estos porcentajes son alarmantes porque la solución lleva meses disponible para los internautas y, a estas alturas, el contagio no debería suponer un problema.

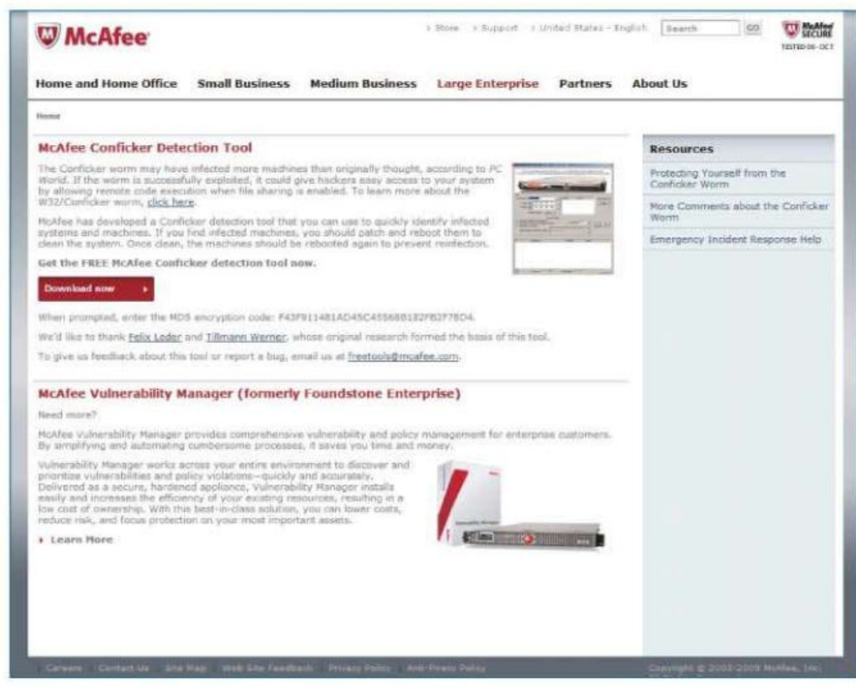
Uno de los factores que han ayudado a que todavía se siga extendiendo es que Conficker ha ido sufriendo algunos cambios durante estos meses y no sólo en su modo de contagio. Por ejemplo, las primeras variantes consultaban un listado de dominios en búsqueda de actualizaciones del malware todos los días y, más adelante, pasaron a utilizar secuencias aleatorias de caracteres para generar los nombres de archivos.

Así es más difícil localizar la infección. Entre las dificultades que presenta su eliminación es que tiene la capacidad de actualizarse automáticamente con cada nueva versión, y gracias a esta capacidad consigue evadir la detección. Además, bloquea el acceso a las páginas web de algunas empresas dedicadas a la seguridad, como las de antivirus y otras soluciones similares, para evitar que el usuario ejecute herramientas de limpieza de su sistema.

Pese a todo ello, ya no es un gusano que suponga un problema grave. Todos los ordenadores con el parche instalado están a salvo de la infección. Si algún usuario no ha llegado a tiempo, también puede solucionarlo fácilmente gracias a las herramientas desarrolladas por los distintos antivirus, que lo eliminan desde el programa instalado en el ordenador e, incluso, desde Internet. Los más atrevidos pueden hasta intentarlo manualmente.



Symantec nos ofrece esta herramienta para limpiar este gusano: http://www.symantec.com/security_response/writeup.jsp?docid=2009-011316-0247-99



Esta es una herramienta específica y gratuita que indica si el equipo está infectado o no: http://www.mcafee.com/us/enterprise/confickertest.html



Un cortafuegos para las aplicaciones web

Para proteger las aplicaciones web de cualquier tipo de ataque no bastará con un firewall o un sistema IDS. La mejor opción posible es adquirir un WAF, un cortafuegos que bloquea las amenazas e inspecciona y auditora el tráfico de HTTP.

Protegerse de los virus que circulan en la Red es una de las obsesiones de cualquier usuario. Pero ¿qué ocurre cuando las amenazas se realizan contra las aplicaciones web? Y es que los ataques contra estos dominios se han convertido en una amenaza muy grande que pone en serio peligro la integridad de los equipos, así como la seguridad de los datos de los usuarios.

No hay que olvidar que las aplicaciones web son unos de los principales focos de ataque de hackers y gusanos, siendo tal vez el punto más vulnerable de las infraestructuras de red. Por lo tanto, de no emplearse medidas se seguridad en lo que se refiere a las transacciones HTTP, HTTPS y FTP, pueden convertirse en uno de los mejores puentes de acceso hacia las redes corporativas y su valiosa información confidencial. Y esto en plena época de expansión web, donde las empresas deben hacer crecer sus servicios en la Red para ofrecer a los clientes una mayor comodidad.

¿Qué aplicaciones no sirven?

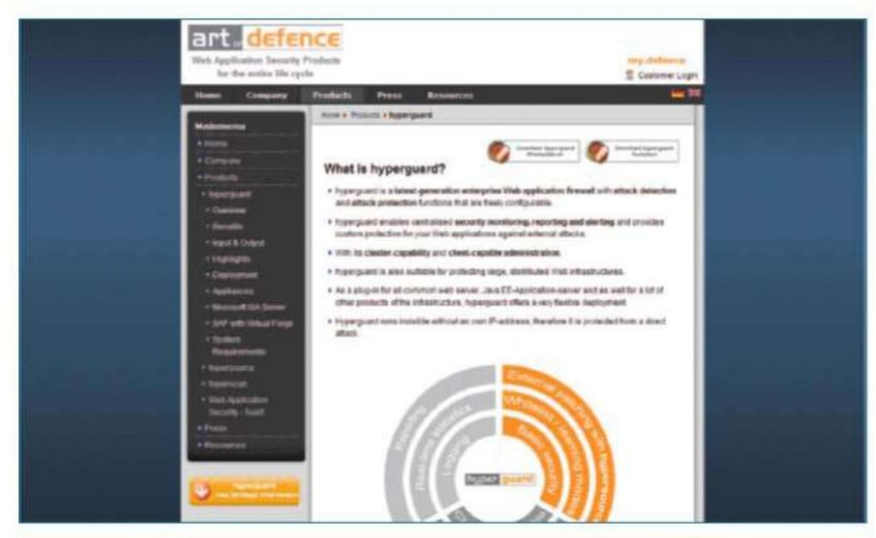
La manera en la que los programas maliciosos se infiltran en las aplicaciones web es a través de los mensajes de los protocolos HTTP/HTTPS. Estos salen al exterior por los puertos 80 y 443 que deja abierto el cortafuegos. Ello no significa, obviamente, que el firewall no sirva de nada. Al contrario, es básico para proteger el equipo de otros ataques como los de denegación de servicio, u otros dirigidos contra otros servicios del servidor web no ofrecidos al exterior. Asimismo, los sistemas IDS (Intrusión Detection System) se centran en la detección de ataques de red monitorizando el tráfico TCP/IP y comprobado que no existen paquetes maliciosos, pero sin analizar en ningún momento el tráfico dentro del protocolo HTTP.

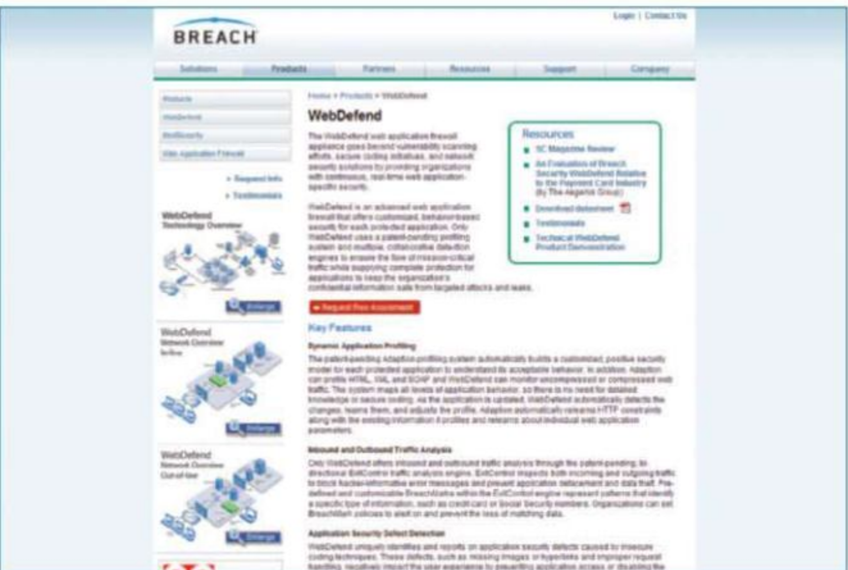
De este modo, pasan también por alto los ataques. ¿Y qué hay de SSL (Secure Socker Layer)? Esta tecnología, que proporciona sus servicios de seguridad cifrando los datos intercambiados entre el Server y el cliente, no impide que aquellas peticiones llegadas al servidor con cifrado SSL contengan ataques. Así pues, sin dejar de resaltar la importancia que tiene para luchar contra los ataques de intercepción o manipulación en el tráfico, no asegura en absoluto el servidor ni la información.

Un proceso de auditoría

Ante esta situación, la única alternativa pasa por implantar la seguridad desde el inicio de vida de la aplicación. Pero el problema radica en que, si bien los administradores sí suelen ser personas formadas en materia de seguridad, no puede decirse lo mismo de los programadores, que normalmente no tienen un gran conocimiento de cuales son las vulnerabilidades con las que puede encontrarse una web no segura. Las deficiencias en materia de protección se producen, en la mayoría de los casos, por un diseño







pobre de la aplicación o de su sistema de codificación. Al no existir un sistema óptimo de valoración de los datos que entran, se facilita mucho la tarea de los hackers. Si bien es cierto que en los últimos años sí se aprecia cierta toma de conciencia de los programadores para con la seguridad de las aplicaciones, hay que tener en cuenta que es un proceso lento y que se presta a errores humanos.

Para identificar las debilidades puede realizarse una auditoría técnica que, hasta hace poco, se veía como el único método realmente viable de lograr proteger aplicaciones web. Sus inconvenientes son que se trata de un proceso muy costoso ya que, generalmente, se debe subcontratar a alguna firma especializada. Y a ello se suma ciertas inseguridades que se derivan a veces de las resoluciones tomadas que, no conviene olvidarlo, son el resultado de análisis llevados a cabo en un momento puntual. Y es que las aplicaciones evolucionan al mismo tiempo que las plataformas y las necesidades de seguridad varían. Como consecuencia de ello, el informe de auditoría va perdiendo vigencia a medida que pasa el tiempo. A ello se suma otra serie de gastos adicionales. A saber, la corrección de las vulnerabilidades localizadas o el tiempo que se emplea en ello. Y mientras se subsanan estos errores, nadie asegura que no vayan a crearse otros nuevos o que todo el esfuerzo sea en balde porque se trate de problemas que provienen de mucho tiempo atrás y fruto del error de programadores que tal vez ya no estén presentes.

WAF: Una solución

En esta coyuntura, cobra fuerza una herramienta que permite ahorrar en costes y ayudar a que las aplicaciones de la Red estén libres de riesgos: se trata de los cortafuegos de aplicaciones web (WAF). La definición que se puede llevar a cabo de esta herramienta es la de un programa que filtra peticiones HTTP/HTTPS que llegan al servidor web de modo que no permitan la entrada a aquellas que puedan considerarse como dañinas, y dejando pasar a todas las demás. Su manera de operar es mediante un proceso automático y de gran fiabilidad que además no

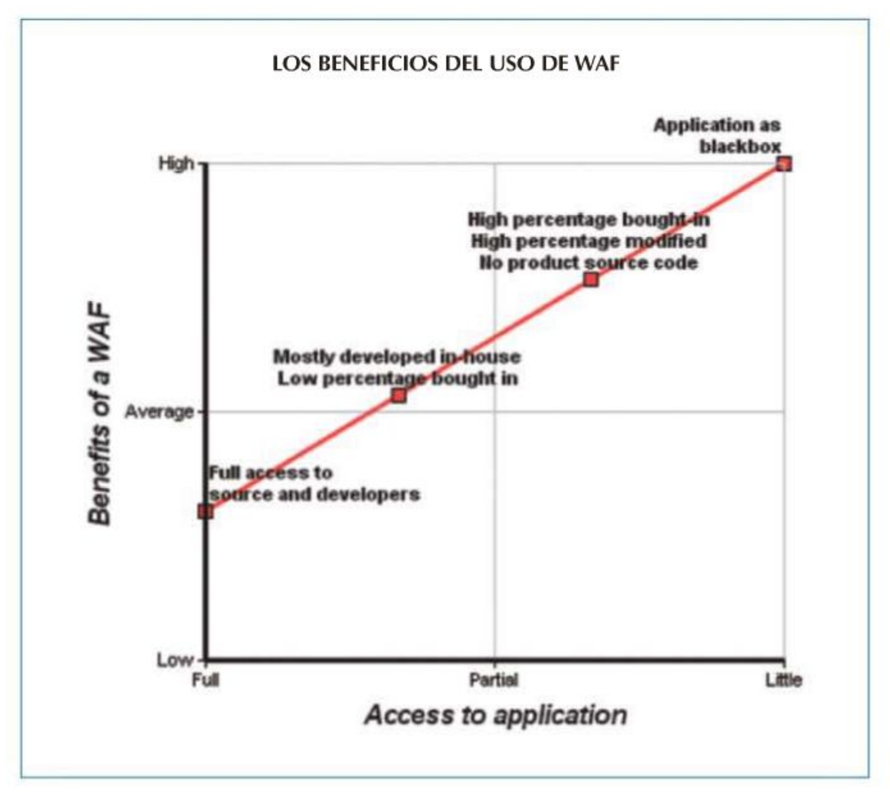
>>> ¿PARA QUÉ SIRVE UN WAF?

Las prestaciones que puede llevar a cabo un programa de este tipo son las siguientes:

- **Inspecciona el tráfico SSL, centrando esta labor criptográfica y entregándola posteriormente al tráfico de los servidores web.**
- **Realiza una auditoría del tráfico HTTP. Permite, a su vez, centralizar el trabajo de varios servidores registrando una gran cantidad de información.**
- **Bloquea ataques en base a unas reglas. Cuando un paquete encaje en una de ellas se considerará una amenaza y la rechazará.**
- **Identifica errores de la aplicación web, tanto los que se manifiestan en el análisis del código fuente como los que sólo se localizan una vez el servidor entra en producción.**
- **Ofrece respuesta a los incidentes. Ya que está especializado en el tráfico HTTP es más fácil registrar más información acerca de las peticiones entrantes.**
- **Identifica los ataques y las vulnerabilidades antes que cualquier otra solución existente.**
- **Es capaz de detectar también información sensible abandonando el servidor web como números de una tarjeta de crédito o DNI, y bloquearlo si así se ha configurado previamente por el usuario.**

requiere la intervención de desarrolladores. Y una vez dicho esto, hay que mencionar que no se trata de una solución única e inamovible, sino que se adapta a las necesidades de cada organización: hardware o software, basada en reglas que definen la firma que realiza los ataques o basadas en la definición de tráfico normal, etcétera.

Se puede hablar de dos tipos principales de arquitectura WAF: como dispositivo de red o como módulo de servidor. En el primer caso, se trata de un dispositivo más conectado a una red. El WAF hace las veces de Proxy inverso (programa o dispositivo que hace las veces de otro) y recibe todo el tráfico que iba dirigido a los servidores web, analizándolo por si contiene algún tipo de riesgo y, en caso negativo, devolviéndolo a la circulación. La principal ventaja con la que cuenta en este caso es la posibilidad de centralizar toda la seguridad en un punto, lo que a su vez permite personalizar el tipo de protección que se desea: aplicar controles de acceso comunes, descifrar comunicaciones SSL y concentrar los registros de auditoría en una máquina. Asimismo, el rendimiento es mayor ya que se evita que sean los propios servidores web los que filtran las peticiones, y se mejora el aspecto de la privacidad, porque al exponerse al exterior las direcciones de los servidores, se usa únicamente la del WAF, que cuenta con una única dirección constante de puertas afuera más allá de los cambios que sucedan dentro de la infraestructura de red. Por otro lado, el inconveniente proviene también de su unicidad como punto de acceso, que puede desembocar en un punto único de fallo. Las soluciones son utilizar dos WAF en aquellos cluster de gran disponibilidad, o uno único funcionando transparentemente con una tarjeta de red dual. De este modo, aun dejando de funcional el WAF el tráfico seguirá atravesando de un puerto a otro.



La segunda opción que se contempla es la de conectarlo a un puerto espejo del conmutador de red, de modo que tenga una copia de todo el tráfico de datos que llegan a través de la Red. Se encarga de hacer un análisis y en caso de detectar algún tipo de programa malicioso, lo registra y reconfigura, a su vez, las reglas del firewall para que impida su entrada al sistema. Su inconveniente principal está claro: al recibir una copia, no es capaz de filtrar los datos antes de que lleguen al servidor sino, tan sólo, asegurarse de que no haya actividad sospechosa en ellos. La mayoría de las veces, WAF funciona como un módulo software especial que sirve para proteger principalmente a un servidor de tipo Apache o ISS.



Un pequeño truco

Protegerse de los virus que circulan en la Red es una de las obsesiones de cualquier usuario. Pero ¿qué ocurre cuando las amenazas se realizan contra las aplicaciones web? Y es que los ataques contra estos dominios se han convertido en una amenaza muy grande que pone en serio peligro la integridad de los equipos, así como la seguridad de los datos de los

usuarios. No hay que olvidar que las aplicaciones web son unos de los principales focos de ataque de hackers y gusanos, siendo tal vez el punto más vulnerable de las infraestructuras de red. Por lo tanto, de no emplearse medidas se seguridad en lo que se refiere a las transacciones HTTP, HTTPS y FTP, pueden convertirse en uno de los mejores puentes de acceso hacia las redes corporativas y su valiosa información confidencial. Y esto en plena época de expansión web, donde las empresas deben hacer crecer sus servicios en la Red para ofrecer a los clientes una mayor comodidad.



¿Qué aplicaciones no sirven?

La manera en la que los programas maliciosos se infiltran en las aplicaciones web es a través de los mensajes de los protocolos HTTP/HTTPS. Estos salen al exterior por los puertos 80 y 443 que deja abierto el cortafuegos. Ello no significa, obviamente, que el firewall no sirva de nada. Al contrario, es básico para proteger el equipo de otros ataques como los de denegación de servicio, u otros dirigidos contra otros servicios del servidor web no ofrecidos al exterior. Asimismo, los sistemas IDS (Intrusión Detection System) se centran en la detección de ataques de red monitorizando el tráfico TCP/IP y comprobado que no existen paquetes maliciosos, pero sin analizar en ningún momento el tráfico dentro del protocolo HTTP. De este modo, pasan también por alto los ataques. ¿Y qué hay de SSL (Secure Socker Layer)? Esta tecnología, que proporciona sus servicios de seguridad cifrando los datos intercambiados entre el Server y el cliente, no impide que aquellas peticiones llegadas al servidor con cifrado SSL contengan ataques. Así pues, sin dejar de resaltar la importancia que tiene para luchar contra los ataques de intercepción o manipulación en el tráfico, no asegura en absoluto el servidor ni la información.

>>> FUNCIONES QUE PUEDE DESEMPEÑAR WAF

Dispositivo de auditoría que controla las transacciones que tienen lugar y, más en concreto, aquellas que se ajustan a los criterios definidos por el administrador.

Dispositivo que controla el acceso y permite a paquetes de datos entrar o no en el servidor web

Cuando funciona integrado en la red ejerce de Proxy inverso, lo que le permite centralizar todo el acceso respecto del exterior, pudiendo mejorar también el rendimiento del sistema.

Un proceso de auditoría

Ante esta situación, la única alternativa pasa por implantar la seguridad desde el inicio de vida de la aplicación. Pero el problema radica en que, si bien los administradores sí suelen ser personas formadas en materia de seguridad, no puede decirse lo mismo de los programadores, que normalmente no tienen un gran conocimiento de cuales son las vulnerabilidades con las que puede encontrarse una web no segura. Las deficiencias en materia de protección se producen, en la mayoría de los casos, por un diseño pobre de la aplicación o de su sistema de codificación. Al no existir un sistema óptimo de valoración de los datos que entran, se facilita mucho la tarea de los hackers. Si bien es cierto que en los últimos años sí se aprecia cierta toma de conciencia de los programadores para con la seguridad de las aplicaciones, hay que tener en cuenta que es un proceso lento y que se presta a errores humanos. Para identificar las debilidades puede realizarse una auditoría técnica que, hasta hace poco, se veía como el único método realmente viable de lograr proteger aplicaciones web. Sus inconvenientes son que se trata de un proceso muy costoso ya que, generalmente, se debe subcontratar a alguna firma especializada. Y a ello se suma ciertas inseguridades que se derivan a veces de las resoluciones tomadas que, no conviene olvidarlo, son el resultado de análisis llevados a cabo en un momento puntual. Y es que las aplicaciones evolucionan al mismo tiempo que las plataformas y las necesidades de seguridad varían. Como consecuencia de ello, el informe de auditoría va perdiendo vigencia a medida que pasa el tiempo. A ello se suma otra serie de gastos adicionales. A saber, la corrección de las vulnerabilidades localizadas o el tiempo que se emplea en ello. Y mientras se subsanan estos errores, nadie asegura que no vayan a crearse otros nuevos o que todo el esfuerzo sea en balde porque se trate de problemas que provienen de mucho tiempo atrás y fruto del error de programadores que tal vez ya no estén presentes.

WAF: Una solución

En esta coyuntura, cobra fuerza una herramienta que permite ahorrar en costes



y ayudar a que las aplicaciones de la Red estén libres de riesgos: se trata de los cortafuegos de aplicaciones web (WAF). La definición que se puede llevar a cabo de esta herramienta es la de un programa que filtra peticiones HTTP/HTTPS que llegan al servidor web de modo que no permitan la entrada a aquellas que puedan considerarse como dañinas, y dejando pasar a todas las demás. Su manera de operar es mediante un proceso automático y de gran fiabilidad que además no requiere la intervención de desarrolladores. Y una vez dicho esto, hay que mencionar que no se trata de una solución única e inamovible, sino que se adapta a las necesidades de cada organización: hardware o software, basada en reglas que definen la firma que realiza los ataques o basadas en la definición de tráfico normal, etcétera.

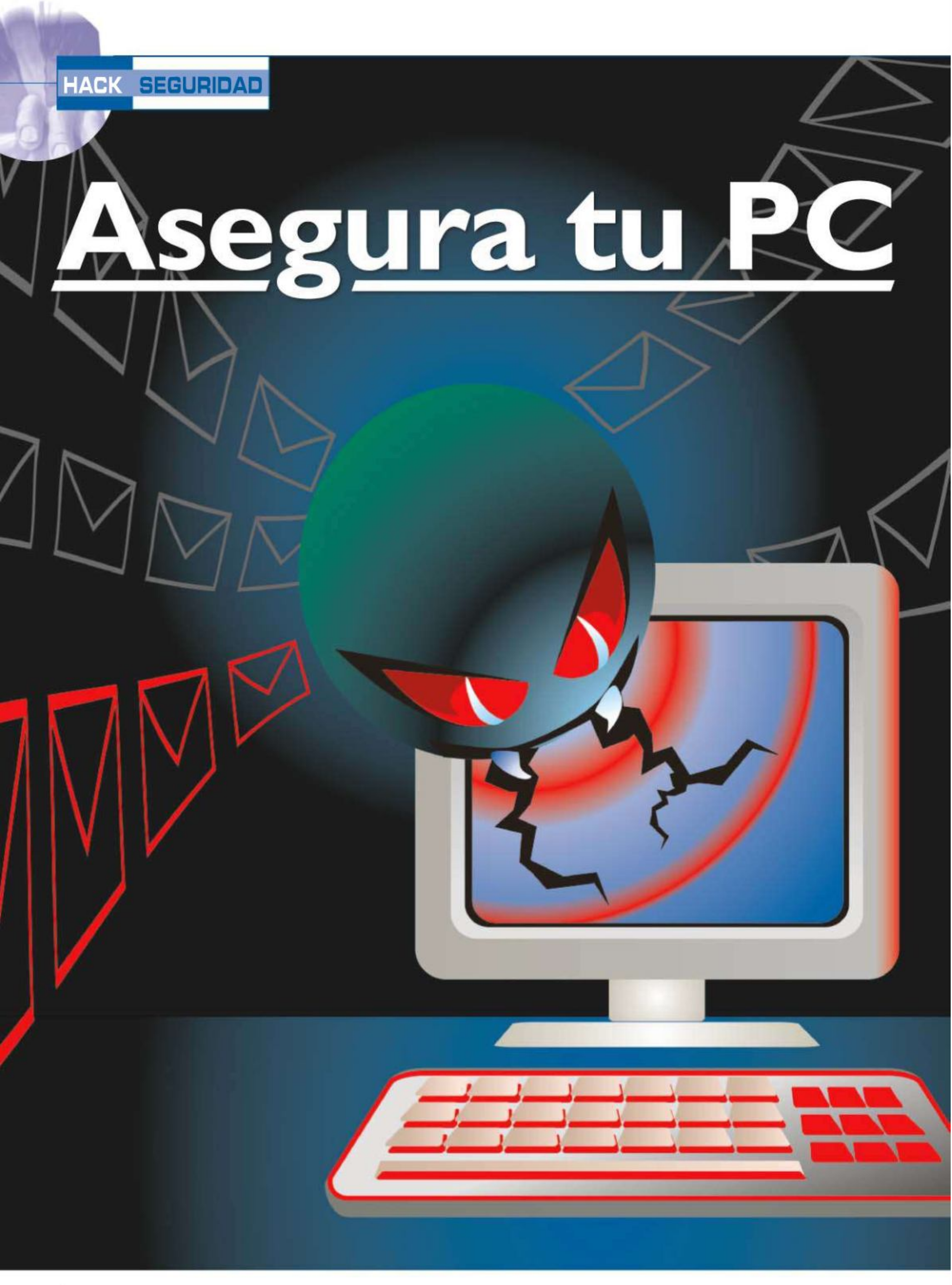
Se puede hablar de dos tipos principales de arquitectura WAF: como dispositivo de red o como módulo de servidor. En el primer caso, se trata de un dispositivo más conectado a una red. El WAF hace las veces de Proxy inverso (programa o dispositivo que hace las veces de otro) y recibe todo el tráfico que iba dirigido a los servidores web, analizándolo por si contiene algún tipo de riesgo y, en caso negativo, devolviéndolo a la circulación. La principal ventaja con la que cuenta en este caso es la posibilidad de centralizar toda la seguridad en un punto, lo que a su vez permite personalizar el tipo de protección que se desea: aplicar controles de acceso comunes, descifrar comunicaciones SSL y concentrar los registros de auditoría en una máquina.

Asimismo, el rendimiento es mayor ya que se evita que sean los propios servidores web los que filtran las peticiones, y se mejora el aspecto de la privacidad, porque al exponerse al exterior las direcciones de los servidores, se usa únicamente la del WAF, que cuenta con una única dirección constante de puertas afuera más allá de los cambios que sucedan dentro de la infraestructura de red. Por otro lado, el inconveniente proviene también de su unicidad como punto de acceso, que puede desembocar en un punto único de fallo. Las soluciones son utilizar dos WAF en aquellos cluster de gran disponibilidad, o uno único funcionando transparentemente con una tarjeta de red dual. De este modo, aun dejando de funcional el WAF el tráfico seguirá atravesando de un puerto a otro.

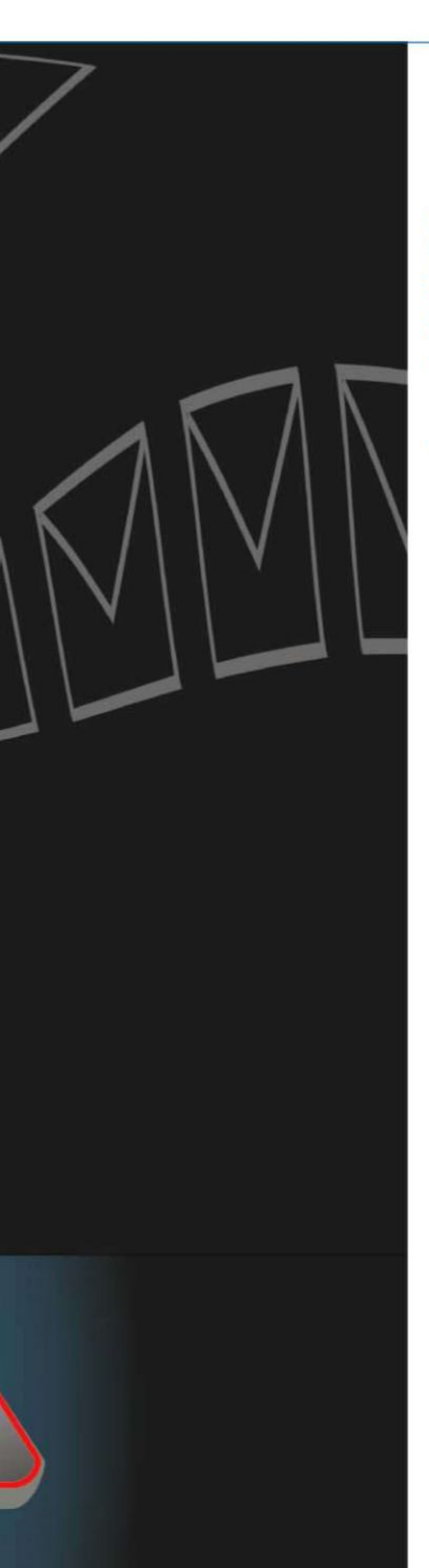
La segunda opción que se contempla es la de conectarlo a un puerto espejo del conmutador de red, de modo que tenga una copia de todo el tráfico de datos que llegan a través de la Red. Se encarga de hacer un análisis y en caso de detectar algún tipo de programa malicioso, lo registra y reconfigura, a su vez, las reglas del firewall para que impida su entrada al sistema. Su inconveniente principal está claro: al recibir una copia, no es capaz de filtrar los datos antes de que lleguen al servidor sino, tan sólo, asegurarse de que no haya actividad sospechosa en ellos. La mayoría de las veces, WAF funciona como un módulo software especial que sirve para proteger principalmente a un servidor de tipo Apache o ISS.






Asegura tu PC





Las soluciones de seguridad son cada vez completas. Protegen del malware, el pishing o el spam y, además, incluyen firewall y control parental. Además, se adelantan a las amenazas gracias a su capacidad proactiva y no ralentizan en exceso el ordenador.

Ocho de cada diez ordenadores tienen algún virus en su sistema. Muchas veces no supone un problema grande, pero cuando se trata de la seguridad del ordenador personal y de todos los datos en él guardados, la cosa es como para tomársela en serio. Si se quiere disponer de las adecuadas medidas de seguridad no basta con un antivirus: los datos no estarán protegidos y muchos ataques no serán neutralizados. Es necesario hacerse con una solución completa que cuente también con la protección de un cortafuegos, antipishing o antispam.

¿Y cuál es la función que cumple cada uno de ellos a la hora de asegurar el sistema? Empecemos por el malware o antivirus: para que sea eficaz tiene que contar con una base de datos amplia que incluya un listado amplio de troyanos, gusanos, programas espía y demás programas maliciosos dirigidos a dañar el sistema. En segundo lugar, conviene hablar de la importancia de contar con un buen firewall o cortafuegos.

Para que pueda hablarse de una buena solución, debe medirse en función de su capacidad para cerrar y esconder los puertos de acceso al equipo, así como resistir el ataque de terceros. Entre sus labores también figuran las de bloquear programas o dominios que, potencialmente, puedan atacar al equipo o a la red. En tercer lugar, se encuentra el sistema antipishing, una solución dirigida a frenar a los estafadores informáticos que intenten adquirir información personal de manera fraudulenta. El delincuente, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea. Para que esto no ocurra, los programas de este tipo se encargan de identificar las amenazas en sitios web y los mails que se reciban. El antispam también desarrolla una labor importante: cataloga como correos basura aquellos que no pertenecen a remitentes autorizados y, asimismo, permite al usuario hacer frente a posibles correos infectados con malware o pishing.

El control parental es otro de los aspectos que más tienen en cuenta las soluciones de seguridad en la Red que se lanzan actualmente al mercado. Puesto que, cada vez más, los ordenadores se encuentran al alcance de los niños, en necesario, de algún modo, controlar cuáles son los sitios por los que pueden navegar y cuáles se les debe prohibir. Las opciones que presentan los últimos productos en este sentido son muy avanzadas, permitiendo programar el ordenador para que no se pueda acceder a determinadas páginas sin introducir antes una contraseña. Finalmente, para prevenirse de que todos los datos guardados en el PC no se pierdan en caso de infección, algunas de estas soluciones cuentan también con la función de Copia de Seguridad.

Implementados

Los sistemas de protección en la Red mejoran año tras año sus prestaciones de seguridad. Un aspecto clave en este sentido es la proactividad: la mayoría funcionan basándose en el comportamiento de amenazas para definir algunas nuevas antes incluso de que sean declaradas como tal. Y también disminuyen la ralentización del equipo cuando se llevan a cabo las actualizaciones. Además, no molestan al usuario mientras disfruta de un videojuego o de una película ya que pueden posponen su labor para más adelante. Asimismo, para no quedar desfasados ante la llegada de Windows 7, muchos antivirus vienen optimizados para funcionar a la perfección en el nuevo sistema operativo de Microsoft.

BITDEFENDER INTERNET SECURITY 2010

Las tecnologías proactivas de las que puede presumir esta solución son muy avanzadas: busca y elimina programas maliciosos ocultos, bloquea Spyware que puedan rastrear las gestiones en la red, y analiza todo el tráfico web, email y mensajería instantánea en tiempo real. Incluye asimismo varias herramientas que se dirigen a proteger la identidad. En este sentido, asegura la información personal frente a filtraciones vía email, y blinda aquellos archivos que almacenan datos personales.

En lo que se refiere a su firewall cuenta con una importante innovación yaque modifica de manera automática su configuración para adecuarse a las circunstancias del entorno. Gracias a ello, el usuario podrá conectarse de manera segura a la red ya esté en su hogar, la oficina o cualquier otro lugar. Por último, para que la navegación de los más pequeños quede supervisada por los padres, bloquea el acceso a páginas web y correos con contenido inapropiado y, también, puede limitar el acceso a determinadas aplicaciones de Internet durante periodos de tiempo que se especifiquen.



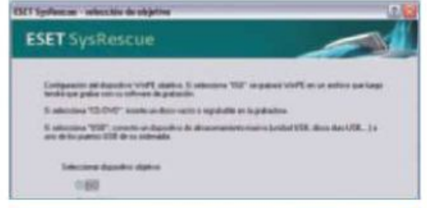


Ficha técnica	
Precio	Para 4 usuarios 82,05 euros
Compatible con	Windows XP, Windows Vista y Windows 7
Página web	www.bitdefender.es

ESET SMART SECURITY 4

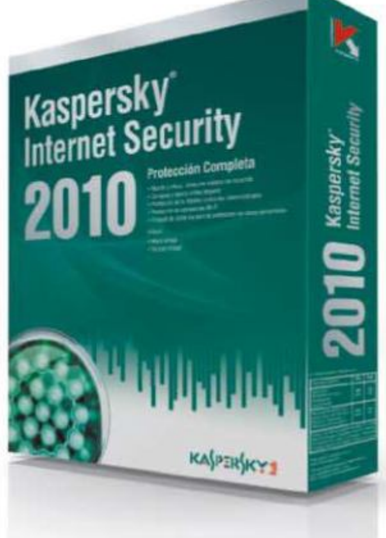
La presencia de la innovadora tecnología ThreatSense es el factor distintivo de este producto: permite la detección proactiva inteligente de malware usando técnicas heurísticas para ayudar a proteger el equipo contra amenazas desconocidas. Además, la firma ha optimizado también el impacto del servicio en el ordenador, garantizando un inicio más rápido y un funcionamiento fluido que disminuye las ralentizaciones. Asimismo, puede destacarse su función de análisis, ya que incorpora características ajustables que permite al usuario establecer la profundidad del análisis, el tiempo máximo del mismo o el tamaño máximo de los archivos comprobados. Dentro del mismo, cuando ESET detecta una infiltración, la clasifica como malware, aplicaciones potencialmente no deseadas o como aplicaciones potencialmente inseguras. En esta versión se ha mejorado la distinción entre ellas utilizando distintos colores de aviso para que así el usuario pueda ver de manera sencilla cual es el nivel de riesgo que existe.

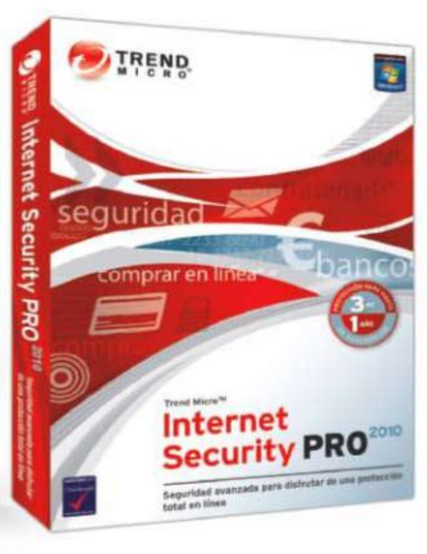
Ficha técnica	
Precio	-
Compatible con	Windows XP y Windows Vista
Página web	www.eset.es













G DATA TOTALCARE 2010

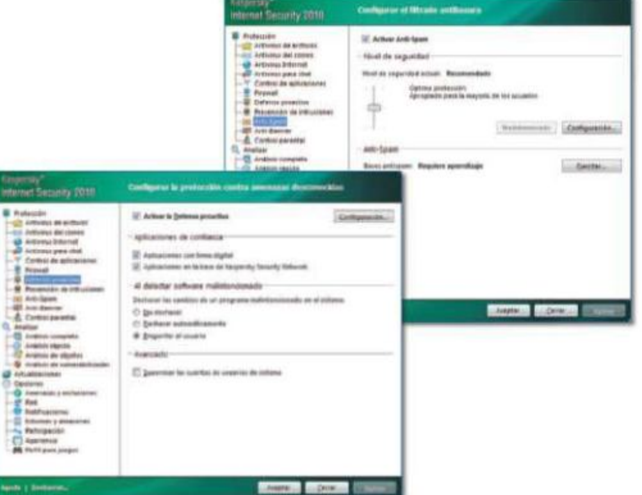
Esta solución completa tiene todo lo que puede pedírsele a un sistema de protección en Internet: antivirus, cortafuegos, copia de seguridad, antispam, antiphising, control parental y optimizador de sistema. Además, gracias a sus dos motores de búsqueda de malware, su rendimiento mejora. Más aun tras cada escaneado, con el que incrementa su velocidad de análisis. Su firewall inteligente también merece ser destacado ya que elimina las interrupciones y ralentizaciones habituales cuando el usuario está llevando a cabo una tarea que requiera el ordenador a pleno funcionamiento. Asimismo, su interfaz mejorada permite ver de manera sencilla cuales son las opciones del usuario, pudiendo acceder a ellas con un solo click. La propia empresa afirma que ha logrado reducir hasta en un 42% el número de clicks necesarios para entrar en las opciones más habituales comprendidas en el menú.



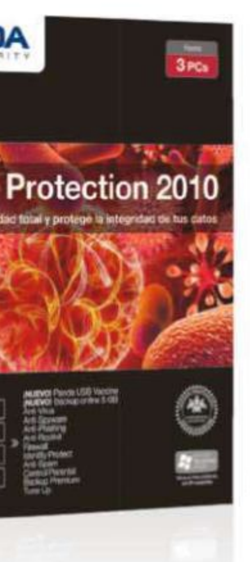
Ficha técnica	
Precio	Para 1 usuario 49,95 euros/ para 3 usuarios: 59,95 euros
Compatible con	Windows XP, Windows Vista, Windows 7
Página web	www.gdata.es

KASPERSKY INTERNET SECURITY 2010

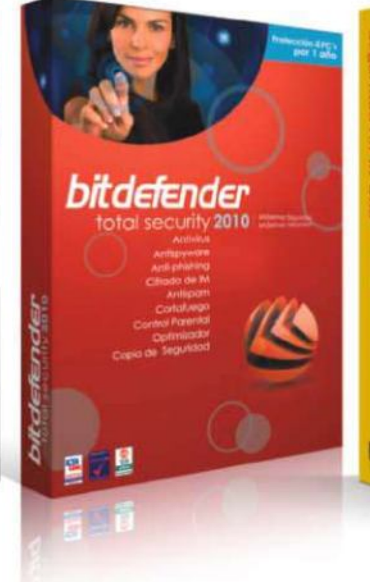
La tecnología Safe Run es una de las principales prestaciones con las que cuenta este producto: gracias a ella es posible una navegación aislada libre de riesgos. Por otra parte, para frenar las amenazas que vengan de la Red, dispone de una aplicación nueva: URL Adivisor, que pone en funcionamiento una barra de color en la parte superior de la ventana cuando una página es considerada peligrosa. Asimismo, para gestionar los derechos de los programas instalados en el propio ordenador, Application Control los organiza en grupos que se basan en cuatro categorías con una serie de derechos y limitaciones al activarse: autorizados, algo restringidos, muy restringidos y totalmente restringidos. Es necesario destacar también la interfaz de usuario: presenta un mayor énfasis en el lenguaje no técnico, separando los principales requerimientos de seguridad de las herramientas más especializadas y facilitando la navegación.

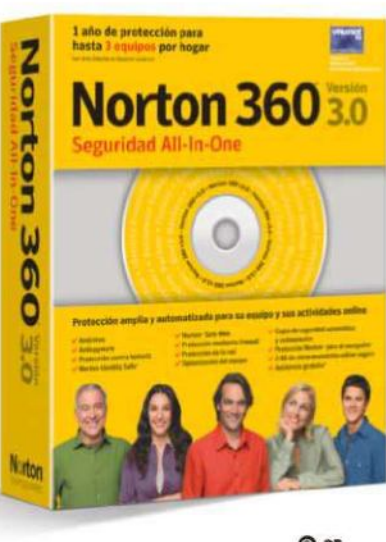


Ficha técnica	
Precio	Para 1 usuario: 49,95 euros/ para 3 usuarios: 69,95 euros/ para 5 usuarios: 99,95 euros
Compatible con	Windows XP y Windows Vista
Página web	www.kaspersky.com









MCAFEE TOTAL PROTECTION 2010

De la mano de la tecnología Active Protection este es una de los sistemas de protección más rápidos frente a amenazas perjudiciales para el equipo. Y es que analiza y bloquea en milisengundos las nuevas amenazas sin que sea necesario esperar a que se lleven a cabo las actualizaciones. Además verifica que no existan amenazas en las zonas del ordenador que sufren ataques con más frecuencia. Gracias a esta rapidez funciona siempre en un segundo plano para permitir al usuario ver vídeos o jugar sin sufrir interrupciones. Otra novedad es el sistema de clasificación de seguridad de sitios web a través de la tecnología McAfee SiteAdvisor. Su labor es la de avisar de las páginas que pueden poner en peligro el equipo o la identidad del usuario utilizando distintos colores en función de la peligrosidad.

Ficha técnica	
Precio	Para tres usuarios 79,95 euros
Compatible con	Windows XP y Windows Vista
Página web	es.mcafee.com



NORTON 360 V3.0

Uno de los aspectos por los que destaca es por la tecnología Norton Safe Web, un servicio de valoración de sitios web que se dirige a ampliar la protección en la Red independientemente de si se encuentra navegando, realizando búsquedas, comprando o interactuando. Su eficacia de búsqueda es tal que el 60% de los sitios que diagnostica como poco seguros, incluyen algún tipo de amenaza. Por otra parte, Norton Identity Safe es una solución que salvaguarda los datos confidenciales gestionando de forma segura las identidades online y almacenando nombres de usuarios y contraseñas para facilitar las compras en la Red, las operaciones bancarias y la navegación. A su vez, impide que se instalen programas espía como aquellos que capturan la información del usuario al registrar las teclas que pulsa. Y para que los datos no se pierdan, la herramienta Norton Backup Drive hace posible gestionar las copias de seguridad. Para terminar, incluye un Smart Startup Manager que desconecta o retrasa aquellos programas innecesarios que reducen la velocidad del tiempo de inicio del sistema.





Ficha técnica	
Precio	89,99 euros
Compatible con	Windows XP, Windows Vista y Windows Vista
Página web	www.symantec.com

>>> SISTEMA DE PROTECCIÓN WINDOWS 7

Windows Vista ofrecía a aquellos que no querían gastar dinero en un programa de seguridad en la red la posibilidad de contar con un sistema de protección gratuita. Gracias a él los usuarios se protegían de cerca del 60% las infecciones de malware existentes. Windows 7 no es menos, y viene incorporado con un completo sistema de protección. Su principal herramienta es Windows Defender, que protege del Spyware y otras formas de software malicioso. Para avisar cuando sea necesario llevar a cabo alguna acción, el Action Center utiliza sus sólidos sistemas de alerta que se benefician de la protección en tiempo real del sistema, que proporciona una monitorización permanente. Cuenta con un sistema firewall que puede complementar a una solución externa ya que permite incorporar a la herramienta del fabricante que se contrate funciones personalizadas. En cuanto al control parental, el nuevo sistema operativo de la firma permite a los padres determinar a qué juegos informáticos pueden acceder sus hijos, qué aplicaciones pueden utilizar y programar cuanto tiempo pueden utilizar el ordenador asegurándose de que no están jugando cuando deberían estar haciendo los deberes. Protección Infantil de Windows Live trabaja paralelamente con el Control Parental para preservar la seguridad de los niños en la Web, filtrando sitios Web inapropiados y proporcionando a los padres informes sobre la actividad de sus hijos en los PCs

>>> ¿CÓMO ADQUIRIRLOS?

Lo normal es que la mayoría de estos productos puedan obtenerse con una o tres licencias. En caso de tener dos o más ordenadores en casa, la segunda opción resultará más económica. La caducidad es de un año, si bien es posible comprarlo por dos obteniendo un mejor precio. Asimismo, si bien es cierto que algunos de los fabricantes como Kaspersky o Panda comercializan sus soluciones en las tiendas, otros muchos sólo lo hacen en Internet. Si se desea, en estos casos, contar además con un CD de instalación, la empresa lo enviará a través de correo pagando en torno a diez euros más.

>>> EXTREMAR PRECAUCIONES

Más allá del sistema de protección en la Red que se utilice, conviene tomar una serie de medidas que eviten que un equipo quede en peligro o que los datos confidenciales estén a la vista de terceras personas.

- Se recomienda no enviar nunca a través de mail datos confidenciales ya que pueden ser interceptados aun tomando medidas de precaución.

- No abrir correos que resulten sospechosos. Si contienen un enlace, aun proviniendo de un contacto conocido, es preferible teclear la dirección en lugar de pulsar en el link.

- Cuando se conecte a través de un ordenador público, hay que tener cuidado de que el nombre de usuario y la contraseña nunca queden guardados.

- A la hora de participar en foros, es preferible utilizar una cuenta de correo distinta de la que se usa habitualmente.

PANDA GLOBAL PROTECTION 2010



El motor de malware de esta aplicación analiza ficheros en tiempo real y, bajo demanda, comprueba el correo electrónico antes de que llegue a la bandeja de entrada, analiza el tráfico de Internet independientemente del navegador y elimina todos los rastros dejados por el spyware en el PC. Para complementar esta labor, cuenta también con un firewall personal autoconfigurado inteligentemente, y con una serie de tecnologías de protección proactivas. Y para que los datos personales se mantengan seguros, los programas antirootkit eliminan aquellos espías que existan en el ordenador de manera silenciosa y que se hayan escabullido de la protección del antivirus. También cuenta con antipishing y antitroyanos bancarios, una prestación que hace posible detectar las amenazas más peligrosas empleadas por los ciber-criminales a la hora de hurtar la identidad. Para gozar de una navegación más segura, incorpora aplicaciones antispam y control parental.

Ficha técnica	
Precio	*Para 1 usuario: 69,96 euros/ para 3 usuarios: 89,95 euros*
Compatible con	*Windows XP y Windows Vista*
Página web	*www.pandasecurity.com*

TREND MICRO INTERNET SECURITY PRO 2010



Las principales ventajas de esta solución son asegurar remotamente los archivos y las carpetas confidenciales en caso de pérdida o robo del equipo, así como comprobar automáticamente la legitimidad de los puntos de accesos Wi-Fi cuando se usa el portátil de viaje. Otra de sus principales funciones es evitar que los ladrones de datos, los virus, el spam en mensajes de texto SMS y otro tipo de malware lleguen al terminal, inspeccionando en tiempo real todas las páginas web que se visitan. Las actualizaciones se llevan a cabo de manera automática y, si se está viendo una película o jugando a un juego, se bloquean para que de este modo no se ralenticen las tareas. Asimismo, optimiza el rendimiento del equipo al reducir el tamaño de los archivos así como el tiempo de exploración en un 20%. También limpia el registro y los archivos temporales.

Ficha técnica	
Precio	*59,95 para tres licencias*
Compatible con	*Windows XP, Windows Vista y Windows 7*
Página web	*www.trendmicro.com*

Cómo funciona Google™

Es una de las páginas más visitadas cada día en Internet y el rey entre los buscadores. Google es capaz de encontrar prácticamente de todo en el universo web, y lo más importante: sus resultados son de calidad. Gran parte de su éxito se lo debe a la tecnología PageRank. ¡Descúbrela!



Búsqueda avanzada
Preferencias
Herramientas del idioma

Buscar con Google | Voy a tener suerte

Buscar en: la Web páginas en español páginas de España

Google.es ofrecido en: català galego euskara

Programas de publicidad - Soluciones Empresariales - Todo acerca de Google - Google.com in English

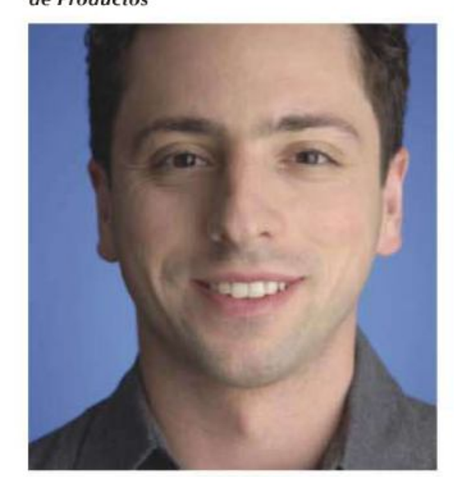
©2009 - Privacidad

Google es el motor de búsqueda por antonomasia en la Red al que cada día millones de internautas de todo el mundo acuden para encontrar toda clase de información: de hecho se calcula que maneja un índice de más de 8.160 millones de páginas web. La pregunta que más de uno se habrá planteado en alguna que otra ocasión es la siguiente: ¿Dónde reside el secreto de su triunfo? ¿Cómo es posible encontrar tan rápido cualquier información que se desea buscar? La clave se encuentra en el término PageRank, una tecnología que permite colocar los resultados más importantes de una búsqueda en los primeros puestos.

Un poco de historia



Larry Page es cofundador y presidente de Productos



Sergey Brin es cofundador y presidente de Tecnología

Los orígenes del buscador tal y como lo conocemos en la actualidad se remontan al año 1995, cuando Larry Page y Sergey Brin, dos estudiantes universitarios de Stanford, comienzan a trabajar en el proyecto "Digital Library" con el propósito de idear un algoritmo para la búsqueda de información. Si Page, ingeniero eléctrico, aportó su experiencia en el diseño web, Brin, licenciado en Informática y Ciencias Matemáticas, hizo lo propio en el área del tratamiento de datos. Este esfuerzo conjunto sirvió para que viese la luz una ecuación matemática vital para el potente motor que comenzaba a forjarse: PageRank, que tiene la habilidad de discernir los sitios de Internet de calidad y con mucho tráfico de aquéllos que son pobres o están dando sus primeros pasos.

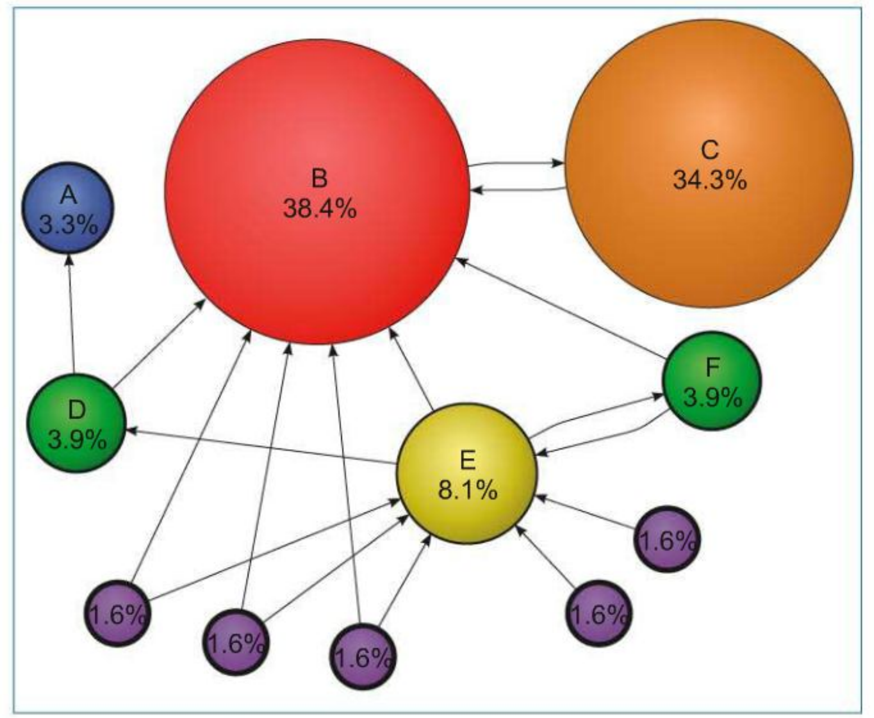
Con la maquinaria engrasada, a principios de 1996 desarrollarían su propio buscador al que denominaron originariamente Backrub. ¿Por qué este nombre? Lo escogieron en alusión a su capacidad de analizar los llamados "back links", es decir los enlaces que dirigen a una página web en concreto. Los primeros usuarios que se beneficiaron de las bondades de BackRub fueron los alumnos y los profesores de propia Stanford. La base de datos manejada por Page y Brin se encontraba alojada, por entonces, en un ordenador Sun Ultra II y tenía un disco duro de 28 Gb de capacidad.

Un año más tarde, Backrub cambiaría su nombre por el de Google que se asemeja bastante al término inglés "googol" (representa el número 10 elevado a la 100 potencia). En la actualidad, el portal presenta una interfaz muy depurada y se consulta en más de 35 idiomas.

PageRank es la clave

Ahondando en la metodología empleada, lo primero que Google hace es rastrear, recolectar y ordenar la información que hay en Internet mediante la ayuda de los web spiders o arañas web. Esta tarea es muy importante porque gracias a ella el buscador se encuentra en condiciones de poder forjar un índice a partir del cual trabajar. De igual forma, en dicho índice sólo van a tenerse en cuenta aquellas direcciones y páginas acordes a unos valores y criterios vinculados a la calidad de sus contenidos.

Una de las arañas más conocidas de Google es Freshbot, que se encarga de recabar y escanear aquellos sitios cuya información se actualiza con bastante frecuencia como son las páginas y los portales de noticias. No obstante, la araña web más antigua de todas, y quizás la más importante, es la del rastreador



Google ordena los resultados de la búsqueda utilizando su propio algoritmo PageRank. A cada página web se le asigna un número en función del número de enlaces de otras páginas que la apuntan, el valor de esas páginas y otros criterios no públicos.

>>> LEVANTANDO UN GRAN IMPERIO

Cuando el 7 de septiembre de 1998, Sergey Brin y Larry Page, dos estudiantes de doctorado de la prestigiosa Universidad de Stanford, fundaban Google Inc., la empresa propietaria de la marca Google, es más que probable que ni ellos mismos supiesen que estaban haciendo historia. Y es que en la actualidad, Google es mucho más que un buscador de información: también tiene un potente motor de fotografías, noticias y vídeos (es propietaria de Youtube) y cuenta con el aval de otros servicios no menos importantes como Gmail (correo electrónico), Google Desktop (para realizar búsquedas en el propio ordenador) o Google Earth (que provee de imágenes tridimensionales de la Tierra).







Googlebot. Su función es la de recopilar todos los enlaces que los internautas posteriormente consultarán cuando efectúen sus búsquedas. A la hora de proceder a esta labor, Googlebot no sólo indexa páginas en código HTML sino que además puede extraer datos de ficheros en otros formatos como DOC, XLS o PDF, entre otros. Así, y una vez que la información se ha recopilado, ésta se ordena y se divide en bloques que quedan repartidos en diferentes equipos: en el momento en que un usuario va a proceder a una búsqueda, estas mismas máquinas se encargarán de investigar e indagar en sus propios índices para mostrar al internauta aquello que busca.

Con un alto nivel de eficacia en los resultados mostrados, el hecho de que una página web u otra aparezca en una determinada posición tiene mucho que ver con ese grado de relevancia concedido por el índice de Google antes citado. Y aunque en esta clasificación tienen cabida diversos criterios como la actualización o las informaciones que se publican, hay uno que resulta mucho más importante y que Google ha bautizado precisamente como PageRank.

Se trata de un sistema de algoritmos tras el cual se esconde una ecuación matemática que asigna numéricamente la importancia de las web que indexa. En este caso PageRank resulta especialmente interesante porque tiene en cuenta los movimientos de los internautas, de manera que si una página recibe muchas visitas su relevancia será mayor respecto a otra que tiene menos. Junto a este volumen de visitas, también se tiene en cuenta los enlaces que hay de una página a otra: es decir, que cuando un sitio redirige a otro el buscador lo que hace es interpretar que la primera de estas páginas está concediendo un voto a la segunda. A este respecto, los votos que emiten los sitios más importantes (y con un PageRank más alto) tienen un valor mayor y, además, ayudan a que otras web pueda alzarse también con la categoría de importante.

Un trabajo constante

Cada vez que Google rastrea Internet con la ayuda de sus herramientas








En las sede de Google los trabajadores cuentan con unas condiciones de trabajo que son la envidia de muchos.

informáticas, para actualizar su particular índice, lo que se encuentra es que de todo ese material entre un 10% y un 20% es contenido nuevo. Por lo tanto, además de añadir información que no tenía a su base de datos, actualiza la que ya tiene conforme a unos criterios establecidos previamente. De igual forma, este trabajo le va a permitir detectar aquellas páginas que han desaparecido ya sea de Internet o de su propio índice como consecuencia de una falta de calidad. Dicha carencia puede deberse a diversos factores: aparición de malware (una vez que este problema se ha solucionado la página en cuestión volvería a estar en Google) o empleo de métodos poco apropiados de los webmaster para escalar posiciones y que su sitio aparezca en los primeros puestos de una búsqueda, entre otros. Por último, Google también conoce el lugar desde el que los internautas efectúan sus búsquedas a través de la dirección IP que identifica a los ordenadores

>>> UNA DE MATEMÁTICAS

La ecuación PageRank responde al siguiente algoritmo matemático:

$$PR(A) = (1 - d) + d * \sum_{i=1}^{n} \frac{PR(i)}{C(i)}$$

A su vez, cada uno de estos valores tiene una lectura concreta:

- **PR(A): Se corresponde con el PageRank de la página A**
- **d: Este factor de amortiguación tiene un valor comprendido entre 0 y 1. Su presencia se justifica en tanto qu las web que no tienen vínculos o enlaces a otras no resulten beneficiadas frente a las que sí los tienen.**
- **PR(i): Son los valores PageRank que tienen cada una de las páginas i que vinculan a A.**
- **C(i): Entendido como el número de enlaces salientes de la página i (sean o no hacia A).**

Esta tecnología que Google emplea se caracteriza por emplear la llamada inteligencia colectiva a la hora de determinar el grado de importancia de una página. Se trata de una valoración subjetiva, exenta de cualquier tipo de intervención humana, porque en la ecuación arriba indicada entran en juego más de 500 millones de variables y 2.000 millones de términos.

Caffeine

En la actualidad, el buscador está trabajando ya en su nuevo motor cuyo nombre en clave es Caffeine. La arquitectura sobre la que se asienta tiene como propósito que los resultados de las búsquedas sean, si cabe, más numerosos, precisos y rápidos. Para ello, los ingenieros del portal están poniendo el acento en incrementar el tamaño de su actual índice y la velocidad a la que los resultados se indexan para aumentar su relevancia y también su exactitud. Para más información, visita la dirección www2.sandbox.google.com.

Los ordenadores son tontos, como le gustaba decir y con toda la razón del mundo a uno de los profesores que tuve en la carrera. Eso sí, hay ciertas cosas que hacen muy, muy bien, y desde luego mucho mejor que nosotros: realizar cálculos a gran velocidad, y almacenar grandes cantidades de datos. Y, precisamente, es por estas características que nos resultan tan útiles. Dado que nuestra aplicación está dedicada a almacenar datos, nos interesa principalmente la segunda característica; aunque también es cierto que, el hecho de utilizar criptografía, implica inevitablemente hacer uso de la primera.

Curso de java útil

jWadalPasswd (IV)

Saludos a todos, y sed bienvenidos una vez más al Curso de Java Útil. El mes pasado comenzamos la habitual entrega del curso solucionando un problema que habíamos dejado planteado el mes anterior; al llegar a la conclusión de que, si usábamos dos algoritmos criptográficos de tipo hash diferentes sobre la misma información (la clave del usuario), no comprometeríamos la seguridad del criptosistema diseñado. Así pues, modificamos la clase "Hash" para que soportara el nuevo algoritmo (Whirlpool), y a continuación diseñamos la clase "Usuario", que nos permite modelar el soporte de múltiples usuarios en nuestro sistema.

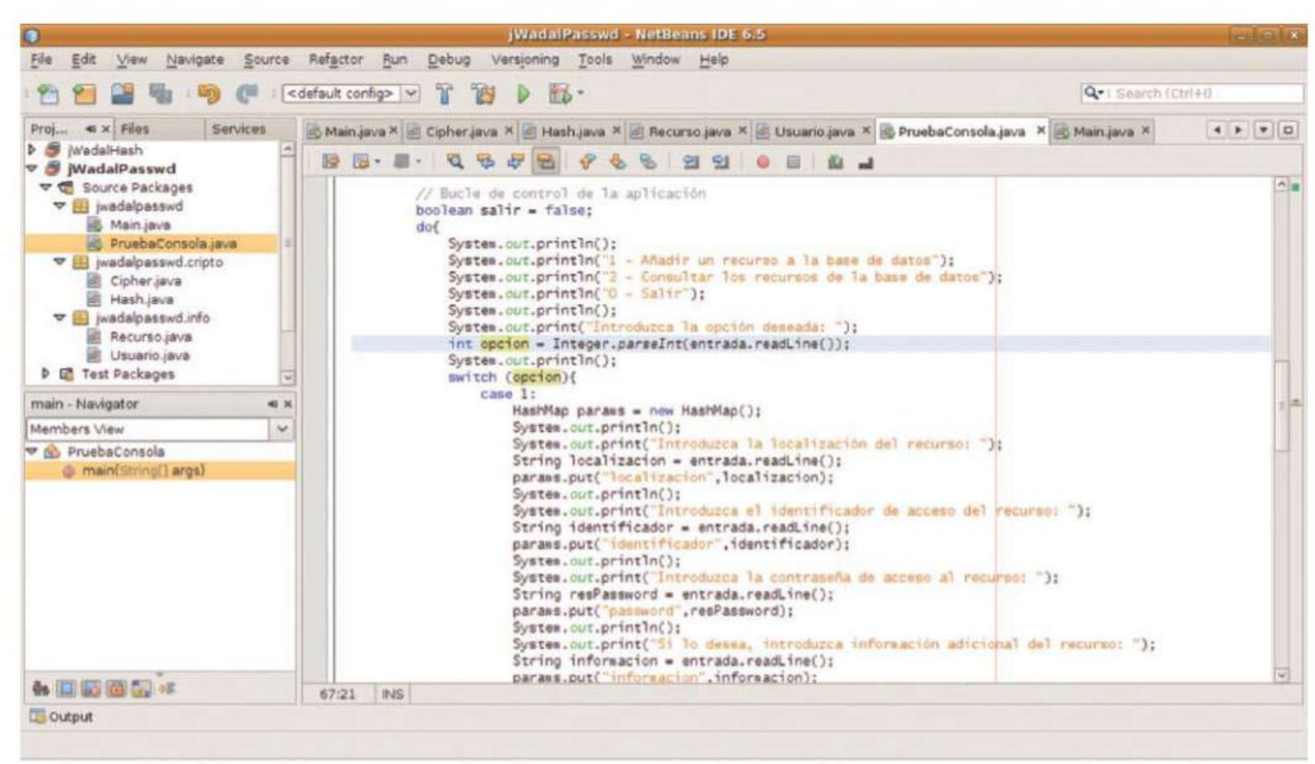
Por último, comenzamos a construir una sencilla interfaz de prueba en consola, con el fin de poder comprobar el funcionamiento del sistema diseñado. Esta última tarea derivó en un interesante inciso teórico sobre algunos aspectos acerca de la memoria dinámica, los punteros, el recolector de basura de la máquina virtual de Java, y demás elementos relacionados.

¿Y los deberes?

Y, si la memoria no me falla, una vez más dejamos en el tintero una pequeña tarea que, supongo, habréis intentado solventar por vuestra cuenta. Se trataba de completar, en el código de la interfaz de prueba de la clase "PruebaConsola", las instrucciones necesarias para diseñar la propia interfaz, atendiendo a cada opción de la estructura de control selectiva "switch" que dejamos esbozada.

En concreto, el bucle que contiene la interfaz de prueba, incluyendo la sección a completar, es el siguiente:

```
// Bucle de control de la
aplicación
boolean salir = false;
do{
  System.out.println();
  System.out.println("1 - Añadir
un recurso a la base de datos");
  System.out.println("2 -
Consultar los recursos de la base
de datos");
  System.out.println("0 -
Salir");
  System.out.println();
  System.out.print("Introduzca la
opción deseada: ");
  int opcion = Integer.
parseInt(entrada.readLine());
  System.out.println();
```



Código de la interfaz de prueba

```
  switch (opcion){
  // ¡COMPLETAR!
  }
  System.out.println();
}
while (!salir);
```

Lo primero que necesitamos, por supuesto, es conocer la sintaxis de la estructura de control "switch".

Esta estructura permite realizar una selección múltiple y exhaustiva sobre tipos de datos que toman valores discretos (char, byte, short e int).

Aunque dicha selección podría sustituirse perfectamente por un conjunto de estructuras "if-then-else" anidadas, la construcción "switch" resulta más clara, elegante, e incluso más eficiente, al no determinar en tiempo de programación la secuencia de comprobación de las expresiones lógicas, y dejar dicho trabajo al compilador. Su sintaxis tiene la siguiente pinta:

```
switch (expresión){
  case constante1:
  //instrucciones
  break;
  case constante2:
  //instrucciones
  break;
  case constanteN:
  //instrucciones
  break;
  default:
  //instrucciones
  break;
}
```

Al evaluar la expresión encerrada entre paréntesis, el compilador busca entre las distintas opciones (delimitadas con la palabra reservada "case") y comprueba si existe una constante con el valor evaluado. Si ésta existe, comienza a ejecutar las instrucciones asociadas a la selección contrastada, y continúa hasta que encuentre una instrucción "break".

En caso de no encontrar ninguna constante que concuerde con el valor evaluado, y sólo en caso de existir, ejecuta las instrucciones asociadas a la selección "default" (por defecto). Es muy, muy importante tener en cuenta el hecho de que se ejecutarán instrucciones hasta encontrar la instrucción "break", pues uno de los errores más típicos es olvidar su inclusión.

En tal caso, y si la constante evaluada es la primera dentro de la estructura de selección, se ejecutarán todas las instrucciones de todas las opciones de forma secuencial.

Añadir un recurso

Una vez sabemos cómo funciona la estructura de control "switch", estamos en condiciones de pasar a implementar nuestra interfaz atendiendo a ella. Como podéis comprobar en el menú impreso por la aplicación, la primera opción corresponde a la adición de un nuevo recurso a la base de datos.

```
case 1:
```

COMENZAMOS A CONSTRUIR UNA SENCILLA INTERFAZ DE PRUEBA EN CONSOLA, CON EL FIN DE PODER COMPROBAR EL FUNCIONAMIENTO DEL SISTEMA DISEÑADO. ESTA ÚLTIMA TAREA DERIVÓ EN UN INTERESANTE INCISO TEÓRICO SOBRE ALGUNOS ASPECTOS ACERCA DE LA MEMORIA DINÁMICA, LOS PUNTEROS, EL RECOLECTOR DE BASURA DE LA MÁQUINA VIRTUAL DE JAVA, Y DEMÁS ELEMENTOS RELACIONADOS.

Por tanto, el primer paso consistirá en instanciar un nuevo HashMap que contenga los parámetros adecuados a dicha operación.

```
HashMap params = new HashMap();
```

A continuación, solicitaremos al usuario los datos sobe el nuevo recurso, los leeremos de la entrada, y los añadiremos al HahsMap de parámetros.

```
System.out.println();
System.out.print("Introduzca la
localización del recurso: ");
String localizacion = entrada.
readLine();
params.put("localizacion",locali
zacion);
System.out.println();
System.out.print("Introduzca
el identificador de acceso del
recurso: ");
String identificador = entrada.
readLine();
params.put("identificador",identi
ficador);
System.out.println();
System.out.print("Introduzca la
contraseña de acceso al recurso:
");
String resPassword = entrada.
readLine();
params.put("password",resPasswo
rd);
System.out.println();
System.out.print("Si lo desea,
introduzca información adicional
del recurso: ");
String informacion = entrada.
readLine();
params.put("informacion",informa
cion);
```

Es el momento de repetir una operación delicada que ya conocemos: la petición de la contraseña al usuario.

Para ello, acudiremos nuevamente a un bucle de lectura que determina la corrección de la contraseña introducida por el usuario, y que será imprescindible para generar el nuevo elemento.

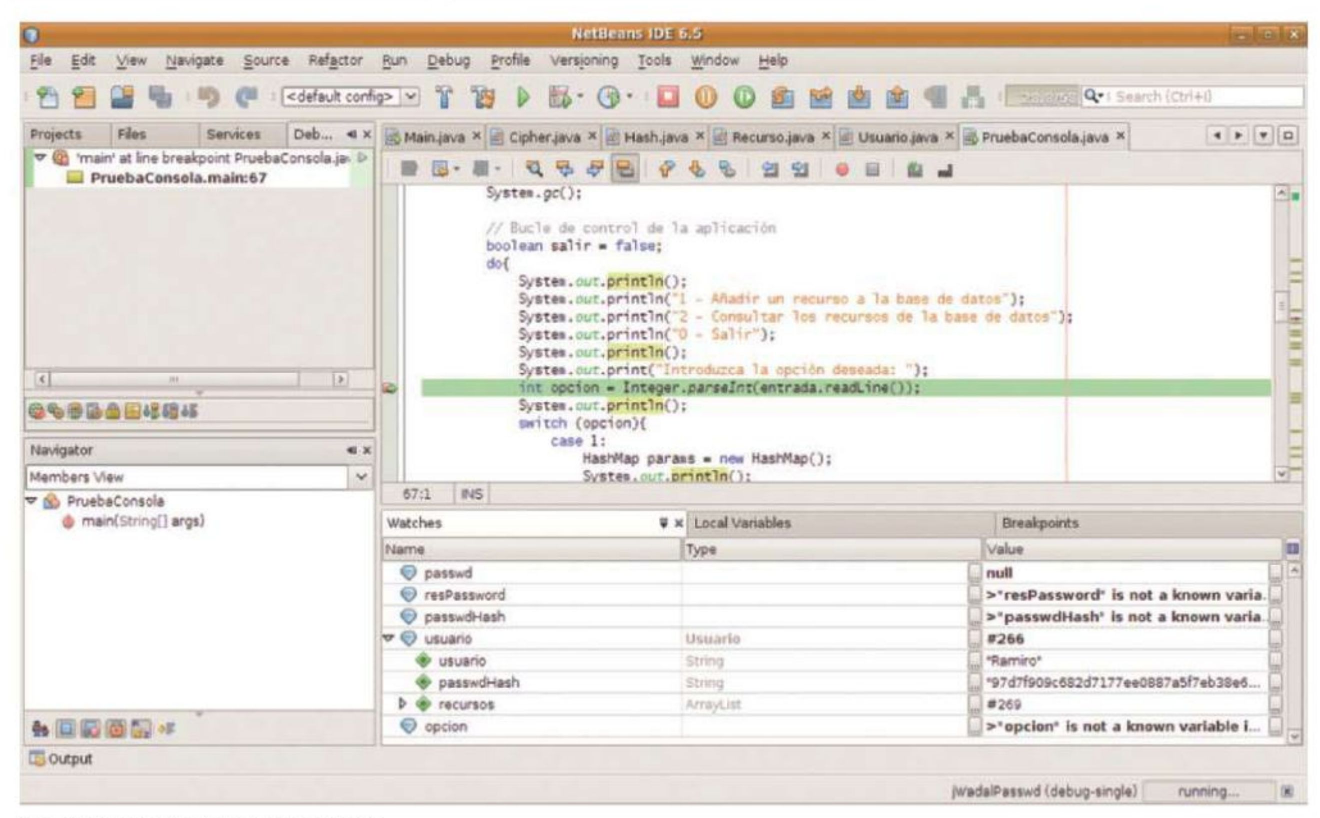
```
continuar = false;
do{
  System.out.println();
  System.out.print("Introduzca su
contraseña: ");
  passwd = entrada.readLine();
  System.out.println();
  if (!usuario.checkPasswd(Hash.
getHashWhirlpool(passwd))){
  System.out.println("¡Contraseña
incorrecta!");
  }
  else continuar = true;
}
while (!continuar);
```

Una vez nos hemos asegurado de que la contraseña es correcta, procedemos a generar el nuevo recurso y asociarlo al usuario.

```
Recurso recurso = new
Recurso(params,Hash.
getHashMD5(passwd));
usuario.addRecurso(recurso);
```

Ahora, y como ya vimos el mes pasado, es imprescindible eliminar de la memoria todo rastro de la contraseña del usuario.

Para ello, desreferenciaremos los objetos que las contienen, y forzaremos la ejecución del recolector de basura de la máquina virtual de Java.



Comprobando el estado de la memoria

```
// IMPORTANTE: desreferenciamos
las contraseñas
resPassword = null;
passwd = null;
// IMPORTANTE: invocamos al
recolector de basura
System.gc();
```

Por último, y con un tratamiento personalizado para recalcar una vez más su importancia, debemos cerrar el bloque de código de la primera selección.

```
break;
```

Consultar los recursos

La segunda opción corresponde a la consulta de los recursos disponibles para el usuario en el sistema.

```
case 2:
```

En este caso, lo primero que debemos hacer es solicitar al usuario su contraseña, de la misma forma que hemos venido haciéndolo hasta ahora, con la petición y comprobación en un bucle de código.

```
System.out.println();
continuar = false;
do{
  System.out.println();
  System.out.print("Introduzca su
contraseña: ");
  passwd = entrada.readLine();
  System.out.println();
  if (!usuario.checkPasswd(Hash.
getHashWhirlpool(passwd))){
  System.out.println("¡Contraseña
incorrecta!");
  }
  else continuar = true;
}
while (!continuar);
```

Una vez nos hemos asegurado de que la contraseña es correcta, calculamos su hash MD5.

```
String passwdHash = Hash.
getHashMD5(passwd);
```

Y, como en anteriores ocasiones, borramos todo rastro de la contraseña del usuario de la memoria.

ESTE MES HEMOS COMPLETADO NUESTRA INTERFAZ DE PRUEBA EN CONSOLA, CON LA QUE HEMOS PODIDO POR FIN COMPROBAR LA VIABILIDAD DE LA ARQUITECTURA DE NUESTRA APLICACIÓN, ASÍ COMO LA CORRECCIÓN DEL CRIPTOSISTEMA PLANTEAD.

```
// IMPORTANTE: desreferenciamos
la contraseña
passwd = null;
// IMPORTANTE: invocamos al
recolector de basura
System.gc();
```

A continuación, obtenemos la lista de recursos del usuario...

```
List<Recurso> recursos = usuario.
getRecursos();
```

... y, tras asegurarnos de que no está vacía...

```
if (recursos.size() < 1){
  System.out.println("¡No hay
recursos!");
}
```

... la recorremos imprimiendo la información de cada recurso.

```
for (Recurso r:recursos){
  System.out.println();
  System.out.
println("Localización: " + r.getL
ocalizacion(passwdHash));
  System.out.
println("Identificador: " + r.getI
dentificador(passwdHash));
  System.out.println("Password: "
+ r.getPassword(passwdHash));
  System.out.println("Información
adicional: " + r.getInformacion
(passwdHash));
}
```

Así mismo, y una vez que deja de ser necesario, eliminamos también de la memoria todo rastro del hash del password, pues se trata de la clave de cifrado de la información.

```
// IMPORTANTE: desreferenciamos
el hash de la contraseña
passwdHash = null;
// IMPORTANTE: invocamos al
recolector de basura
System.gc();
System.out.println();
```

Por último, y recalcando su importancia una vez más, delimitamos el fin del bloque de la selección.

```
break;
```

Últimas opciones y prueba de fuego

Al fijarnos en el menú que creamos, vemos que aún nos falta una tercera opción, que es la de salir del sistema. Ésta es fácil.

```
case 0:
  salir = true;
  System.out.println();
  System.out.print("Saliendo de
la aplicación...");
  break;
```

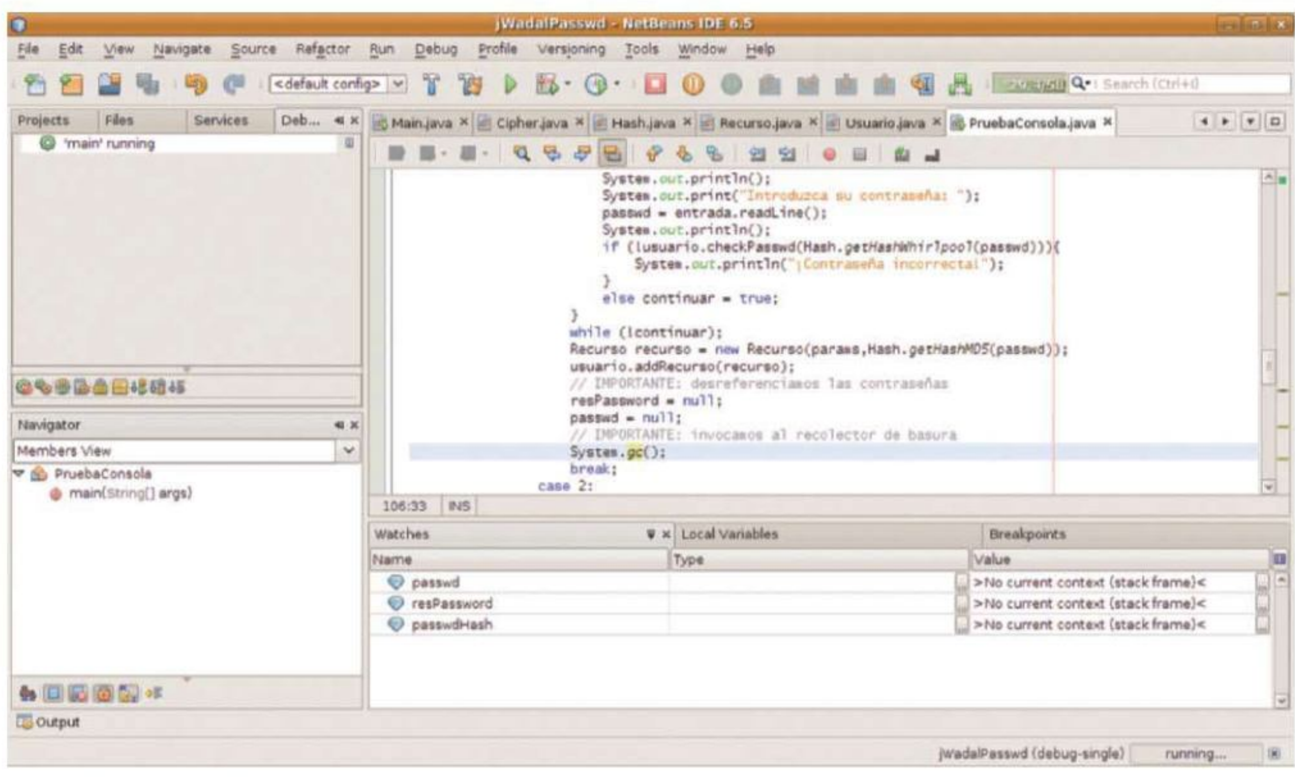
Por supuesto, falta una "cuarta opción" implícita a las estructuras de control "switch", que es la "default", y que en nuestro caso servirá para filtrar entradas no deseadas en el menú de selección.

```
default:
  System.out.println("¡La opción
introducida no es válida!");
  continue;
```

Bien, ha llegado el momento de comprobar el funcionamiento de nuestra interfaz...

```
init:
deps-jar:
compile-single:
run-single:

Introduzca el nombre del nuevo
usuario:
Ramiro
Introduzca la contraseña del
usuario:
prueba
Repita la contraseña del usuario:
prueba
1 - Añadir un recurso a la base
de datos
```



Depurando nuestra interfaz

```
2 - Consultar los recursos de la
base de datos
0 - Salir

Introduzca la opción deseada:
1
Introduzca la localización del
recurso:
http://www.google.es/
Introduzca el identificador de
acceso del recurso: ramiro

Introduzca la contraseña de
acceso al recurso:
contraseña_de_google
Si lo desea, introduzca
información adicional del
recurso:
-
Introduzca su contraseña:
prueba

1 - Añadir un recurso a la base
de datos
```

```
2 - Consultar los recursos de la
base de datos
0 - Salir

Introduzca la opción deseada: 1
Introduzca la localización del
recurso:
http://www.hotmail.com/

Introduzca el identificador de
acceso del recurso:
ramiro

Introduzca la contraseña de
acceso al recurso: contraseña_de_
hotmail

Si lo desea, introduzca
información adicional del
recurso:
-
Introduzca su contraseña:
1 - Añadir un recurso a la base
de datos
```

```
2 - Consultar los recursos de la
base de datos
0 - Salir
prueba
Introduzca la opción deseada:

2
Introduzca su contraseña:

Localización: http://www.google.
es/
Identificador: ramiro
Password: contraseña_de_google
Información adicional: -

Localización: http://www.hotmail.
com/
Identificador: ramiro
Password: contraseña_de_hotmail
Información adicional: -
prueba

1 - Añadir un recurso a la base
de datos
2 - Consultar los recursos de la
base de datos
0 - Salir


Introduzca la opción deseada:
```

COMO PODEMOS COMPROBAR, Y A EXCEPCIÓN DE LOS MOMENTOS EN QUE DICHOS DATOS ESTÁN SIENDO UTILIZADOS EN ALGÚN PROCESO CRÍTICO DE LA APLICACIÓN, LAS VARIABLES CONTENDRÁN VALORES NULOS ("NULL") O NO ESTARÁN DEFINIDAS PARA EL CONTEXTO DE EJECUCIÓN QUE ESTAMOS COMPROBANDO.

```
Saliendo de la aplicación...
0
BUILD SUCCESSFUL (total time: 1
minute 7 seconds)
```

Por lo que parece, todo funciona perfectamente.

¿Hay alguien ahí?

Una y otra vez, a lo largo del presente artículo y el anterior, hemos insistido en repetidas ocasiones en la importancia de que los datos sensibles desaparezcan de la memoria del sistema.

En este caso, consideramos que los datos sensibles son la contraseña del usuario, el hash en MD5 de dicha contraseña (la clave de cifrado), y en menor medida, el hash Whirlpool de la contraseña, usado en el proceso de verificación de credenciales.

Ahora, y sirviéndonos de la rudimentaria interfaz en consola que hemos creado, vamos a comprobar qué está pasando en la memoria del ordenador durante la ejecución de nuestro código. Lo que haremos será ejecutar la interfaz en modo de depurado, utilizando la opción de "Debug".

Una vez estemos ejecutando la aplicación, crearemos "watches" para las variables que almacenan los objetos con la información anteriormente descrita como sensible, y observaremos el contenido de las mismas mientras dura la ejecución del programa. Si no nos hemos equivocado, los datos sensibles deberían permanecer en memoria el menor tiempo posible.

Como podemos comprobar, y a excepción de los momentos en que dichos datos están siendo utilizados en algún proceso crítico de la aplicación, las variables contendrán valores nulos ("null") o no estarán definidas para el contexto de ejecución que estamos comprobando (porque no se utilicen en dicha sección de código).

Para que probéis este aspecto, dejo como pequeña tarea el buscar zonas del código donde dichos datos estén disponibles de forma innecesaria, suponiendo por tanto un riesgo de seguridad para la aplicación.

El mes que viene

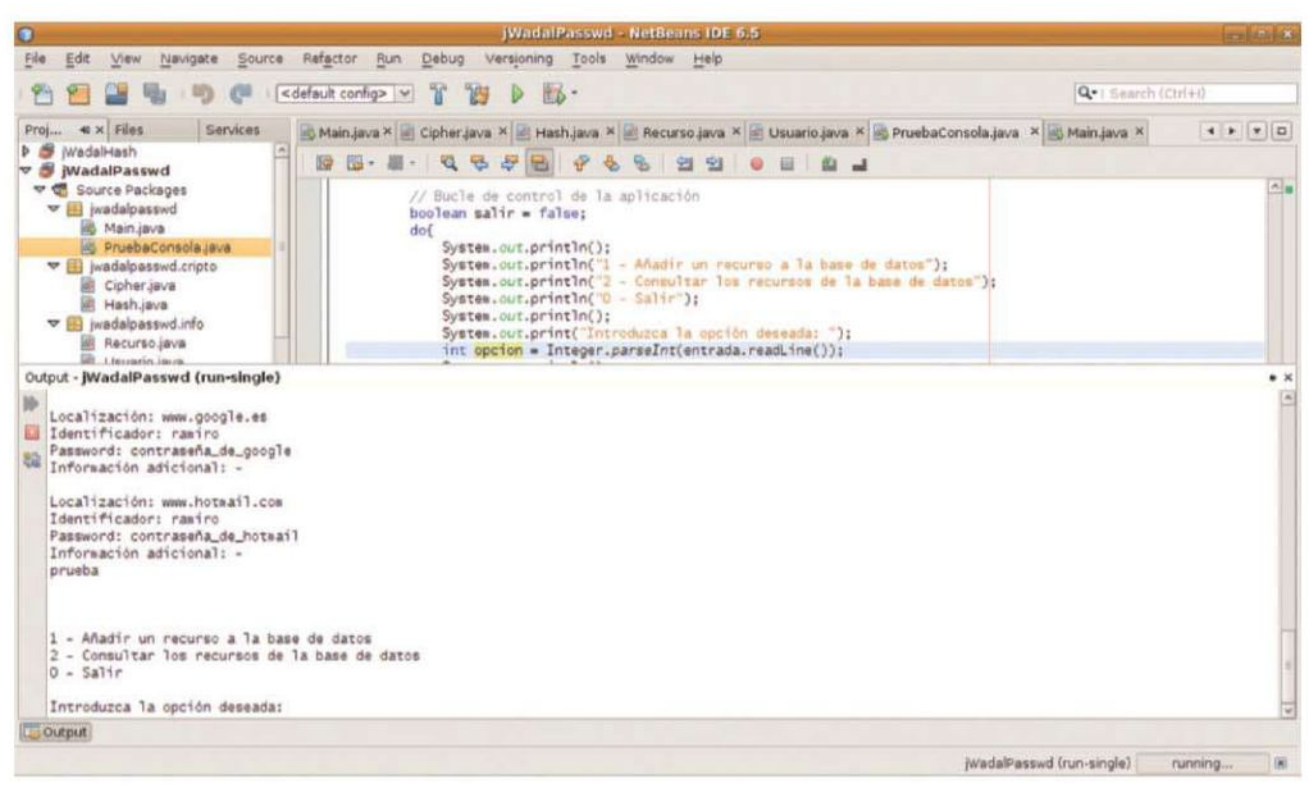
Este mes hemos completado nuestra interfaz de prueba en consola, con la que hemos podido por fin comprobar la viabilidad de la arquitectura de nuestra aplicación, así como la corrección del criptosistema planteado. Además, hemos aprendido a manejar la estructura de control selectiva "switch", y hemos visto cómo utilizar las herramientas de depuración del entorno NetBeans para controlar qué datos se encuentran en memoria en cada momento del ciclo de vida de la aplicación.

El mes que viene continuaremos trabajando en la implementación de nuestra aplicación, incluyendo soporte para almacenar de forma persistente la información de la aplicación en ficheros. Hablaremos de distintas formas para hacerlo, y analizaremos las ventajas e inconvenientes de cada una de ellas.

Como ya sabéis, en mi blog podéis encontrar el código fuente del curso; y mi correo electrónico está a vuestra disposición para preguntas, sugerencias y dudas acerca de los artículos que queráis plantear.

¡Hasta el mes que viene!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/



Interfaz de prueba en consola

En ocasiones, y a pesar de la cantidad casi ilimitada de opciones que nos ofrece el software libre, no encontramos aquella que termina de cumplir con todas nuestras expectativas. Hablo de esa aplicación que hace "casi" lo que nosotros queremos, de ese software al que le falta algún detalle que, para nosotros, lo haría perfecto. Pero, una vez más, la magia del software libre acude en nuestra ayuda: si no existe... ¡siempre podemos crearlo!



Joomla a tu medida

¿No te gusta lo que hay? ¡Pues hazlo tú mejor!

Saludos a todos una vez más. Creo que no será necesario que os describa a vosotros, lectores de esta publicación, todas y cada una de las bondades del software libre; estoy seguro de que conoceréis la mayoría, por unos u otros motivos. Entre ellas, y desde el punto de vista eminentemente técnico, encontramos la disponibilidad del código fuente del software que utilizamos. Este hecho abre la puerta a un vasto abanico de posibilidades en lo que a la personalización se refiere.

Joomla

El software Joomla es un CMS libre (bajo licencia General Public License de GNU) escrito mayoritariamente en PHP, y que surgió en septiembre de 2005 como una escisión del proyecto Mambo, debido a una serie de desavenencias entre un grupo de programadores y la corporación australiana Miro. Actualmente, Joomla es uno de los gestores de contenidos más extendidos y utilizados en Internet, en gran parte debido a su flexibilidad y capacidad de personalización.

En la revista @RROBA hemos hablado de Joomla en varias ocasiones. En el número 135 (diciembre de 2008), escribí un artículo titulado "Despliegue de un CMS Joomla", en el que aprendíamos a instalar y configurar el sistema Joomla, así como todos los servidores necesarios asociados. Al mes siguiente, en el número 136 (enero de 2009), escribí otro artículo titulado "Personalizando Joomla!", en el que aprendíamos a gestionar el sistema de extensiones de Joomla, viendo ejemplos concretos de algunos

elementos adicionales que nos permitían añadir o modificar ciertas funcionalidades del CMS. Además, y durante varios meses, otros compañeros de la publicación han estado estudiando la seguridad de Joomla desde diversos puntos de vista.

Sabemos, por tanto, cómo desplegar el servidor, cómo gestionar sus complementos, y cómo funciona su sistema de seguridad, e incluso ciertos puntos débiles de determinadas versiones que contienen fallos de seguridad. Pero, como comentábamos en la introducción, en ocasiones nos encontramos con que nos falta "algo". Ese pequeño detalle, esa simple funcionalidad.

Por tanto, y para que podáis personalizar vuestro sistema Joomla, pero esta vez con todas las de la ley, vamos a aprender a programar nuestras propias extensiones para el sistema. ¡Vamos allá!

Instalar Joomla

Aunque presupongo que todos sabréis instalar Joomla y los servicios necesarios para hacerlo funcionar (servidor web, servidor FTP, servidor SQL y lenguaje PHP), no está de más hacer un pequeño repaso, sólo por si acaso. Si necesitarais información más detallada, más allá de la pequeña guía de referencia que podréis encontrar a continuación, podéis echar un vistazo a algún tutorial o guía en Internet, así como acudir a los artículos anteriormente mencionados, y publicados en esta misma revista. Por último, comentar que el entorno sobre el que desarrollaremos el trabajo del presente artículo es un sistema Ubuntu GNU/Linux 9.04, ejecutado sobre una máquina virtual.

El primer paso es la instalación del servidor Web, en nuestro caso un sistema Apache2.

```
ramiro@ubuntu:~$ sudo apt-get
install apache2
[sudo] password for ramiro:
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
Se instalarán los siguientes
paquetes extras:
 apache2-mpm-worker apache2-
utils apache2.2-common libapr1
libaprutil1 libmysqlclient15off
libpq5 mysql-common
Paquetes sugeridos:
 apache2-doc apache2-suexec
apache2-suexec-custom
Se instalarán los siguientes
paquetes NUEVOS:
 apache2 apache2-mpm-worker
apache2-utils apache2.2-
common libapr1 libaprutil1
libmysqlclient15off libpq5 mysql-
common
0 actualizados, 9 se instalarán,
0 para eliminar y 0 no
actualizados.
Necesito descargar 3608kB de
archivos.
Se utilizarán 10,3MB de espacio
de disco adicional después de
esta operación.
¿Desea continuar [S/n]?
[...]
```

Tras la instalación, y una vez hayamos comprobado que los módulos del servidor se han habilitado correctamente (veremos varios mensajes del tipo "Enabling module..."), debemos instalar el soporte para el lenguaje PHP.

```
ramiro@ubuntu:~$ sudo apt-get
install php5
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
Se instalarán los siguientes
paquetes extras:
 apache2-mpm-prefork libapache2-
mod-php5 php5-common
Paquetes sugeridos:
 php-pear
Los siguientes paquetes se
ELIMINARÁN:
 apache2-mpm-worker
Se instalarán los siguientes
paquetes NUEVOS:
 apache2-mpm-prefork libapache2-
mod-php5 php5 php5-common
0 actualizados, 4 se instalarán,
1 para eliminar y 0 no
actualizados.
Necesito descargar 3092kB de
archivos.
Se utilizarán 6308kB de espacio
de disco adicional después de
esta operación.
¿Desea continuar [S/n]?
[...]
```

El siguiente paso comprende la instalación del servidor de bases de datos MySQL.

```
ramiro@ubuntu:~$ sudo apt-get
install mysql-server-5.0
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado...
Hecho
Se instalarán los siguientes
paquetes extras:
 libdbd-mysql-perl libdbi-perl
libnet-daemon-perl libplrpc-perl
mysql-client-5.0 mysql-server-core-
5.0
Paquetes sugeridos:
 dbishell mysql-doc-5.0 tinyca
mailx
Se instalarán los siguientes
paquetes NUEVOS:
 libdbd-mysql-perl libdbi-perl
libnet-daemon-perl libplrpc-perl
mysql-client-5.0 mysql-server-5.0
mysql-server-core-5.0
0 actualizados, 7 se instalarán, 0
para eliminar y 0 no actualizados.
Necesito descargar 35,8MB de
archivos.
Se utilizarán 110MB de espacio de
disco adicional después de esta
operación.
¿Desea continuar [S/n]?
[...]
```

Una vez instalado, y tras tomar buena nota de la contraseña configurada para el usuario "root" del servidor, instalaremos el soporte para conectar el lenguaje PHP con el servidor MySQL recién configurado.

```
ramiro@ubuntu:~$ sudo apt-get
install php5-mysql
Leyendo lista de paquetes...
Hecho
Creando árbol de dependencias
Leyendo la información de
estado... Hecho
Se instalarán los siguientes
paquetes NUEVOS:
 php5-mysql
0 actualizados, 1 se instalarán,
0 para eliminar y 0 no actualizados.
Necesito descargar 66,0kB de
archivos.
Se utilizarán 246kB de espacio de
disco adicional después de esta
operación.
[...]
```

El último paso consiste en reiniciar el servidor web Apache.

```
ramiro@ubuntu:~$ sudo /etc/init.
d/apache2 restart
 * Restarting web server apache2
 ... waiting
 [ OK ]
 ramiro@ubuntu:~$
```

Opcionalmente, es recomendable (aunque no imprescindible para el trabajo que desarrollaremos en este artículo) instalar un servidor FTP, como vsftpd, así como crear un usuario específico para el CMS, de forma que sea posible la subida e instalación automática de extensiones de Joomla mediante el sistema de administración del propio software. No detallaré los pasos a seguir, al no ser imprescindible y ser un proceso relativamente largo.

Así pues, sólo restaría descargar el paquete con la última versión de Joomla de la página web oficial (http://www.joomla.org/), descomprimirlo en el directorio "/var/www" y llevar a cabo la instalación del script mediante el asistente del propio CMS.

Extensiones en Joomla

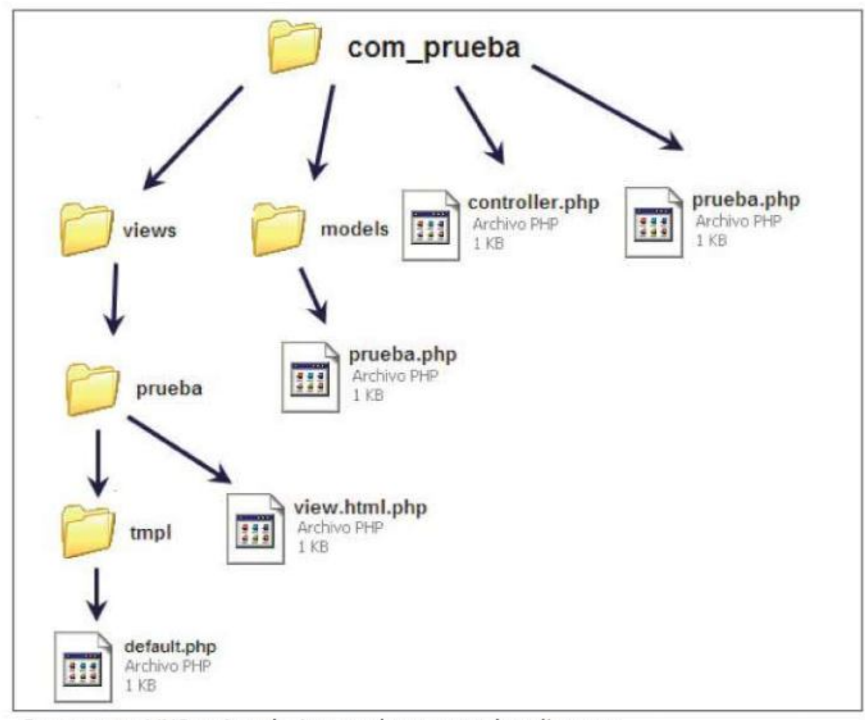
Lo primero que debemos tener en cuenta cuando hablamos de extensiones de Joomla (ojo, de Joomla 1.5, la versión reescrita "from scratch" en PHP5), es que existen tres tipos de ellas bien diferenciados: componentes, módulos y plugins.

El primer tipo de extensión, los componentes, pueden ser considerados aplicaciones en sí mismas. Típicamente se muestran en la parte central de la aplicación web, ocupando por tanto la mayor parte de la atención del usuario. Desde el punto de vista de la funcionalidad, se comportan como aplicaciones independientes, al contener su propia base de información y su sistema de representación independientes. Como suele comentarse en la literatura sobre el desarrollo de componentes para Joomla, "instalar un componente es añadir una aplicación a tu entorno web". Algunos ejemplos de funcionalidad presente en componentes serían foros, sistemas de noticias, galerías de fotografías, etc.

El segundo tipo de extensión, los módulos, son elementos pensados para extender la funcionalidad del portal principal, al mostrar de una forma distinta cierta información ya existente en el entorno de la aplicación. Ciertamente, permiten añadir funcionalidad al sistema, pero no poseen su propia base de conocimiento para generar información, sino que adoptan la existente en el entorno de Joomla. Por poner nuevamente ejemplos, podríamos hablar de las últimas noticias publicadas, estadísticas sobre el sistema, el acceso al propio sistema (login), etc.

Por último, el tercer tipo de extensión, los plugins (los antiguos "mambots" de Joomla 1.0), son algo más "peculiares" que sus otros hermanos. Un plugin actúa como una función que es ejecutada sobre alguna parte de Joomla antes de que ésta se muestre. Esto es, virtualmente cualquier código de Joomla (bien se trate del núcleo, un módulo o un componente) puede ver su comportamiento modificado por un plugin que esté "escuchando" dicha acción para interceptarla y modificarla según haya sido programado. Pongamos un ejemplo. Imaginad un plugin que empotre previsualizaciones de vídeos de youtube en los enlaces que se inserten en las noticias de Joomla.

De esta forma, cuando en una noticia aparece una URL de la forma "http://www.youtube.com/watch?v=...", y cuando ésta vaya a mostrarse en el CMS, el plugin procesará dicha URL y cargará al final de la noticia la previsualización del vídeo con el código HTML correspondiente. Este código HTML no se encuentra en la noticia, sino que es generado bajo demanda por el plugin. Potente, ¿verdad? Sus posibilidades son muy elevadas...



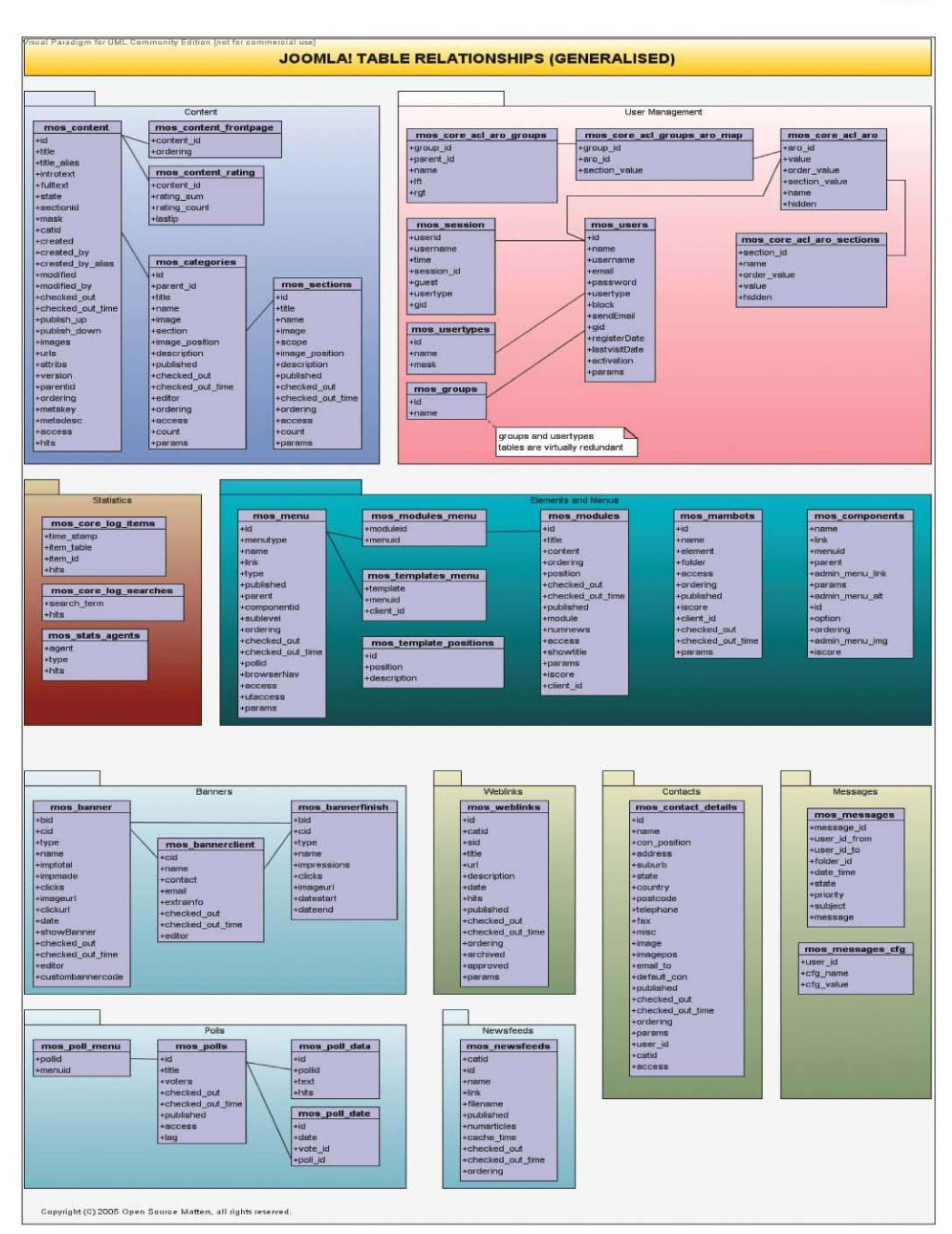
Componente MVC en Joomla. Imagen de www.nosolocodigo.com

El patrón Modelo Vista Controlador

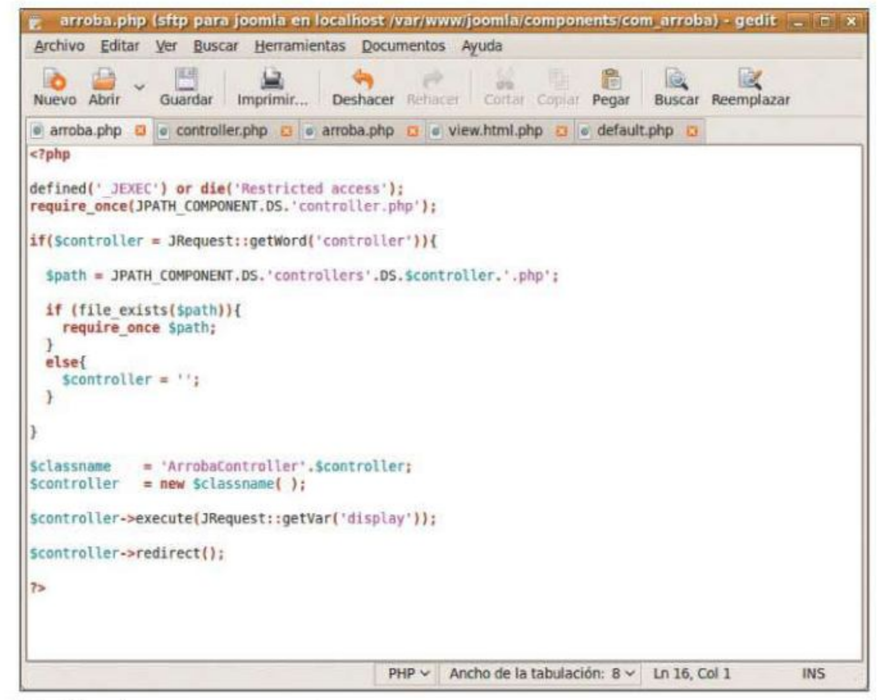
Una de las novedades introducidas en la versión 1.5 de Joomla es la posibilidad de desarrollar sus componentes siguiendo el patrón MVC, también conocido como Modelo Vista Controlador (en inglés "Model View Controller"). Este patrón de arquitectura de software tiene como principal filosofía la separación de los datos de una aplicación, su interfaz de usuario, y su lógica de control.

Aunque no es obligatoria la utilización de estos patrones en el desarrollo de componentes para Joomla, sí resulta bastante conveniente, para ajustarse a las convenciones existentes en este terreno. Por tanto, nosotros vamos a ver cómo desarrollar un componente siguiendo el patrón MVC. Pero antes, por supuesto, vamos a hablar un poco de los elementos de dicho patrón.

El primer elemento de MVC es el modelo, encargado de gestionar los datos de la aplicación. Entre los cometidos del modelo



Arquitectura interna de Joomla



El código de nuestro componente

encontramos el propio acceso a datos (de cualquier tipo: base de datos, servicios web, etc.), la validación de los mismos (comprobación de valores erróneos) y la lógica de programación (cómputos sobre los datos).

El segundo elemento es la vista, que se encarga de presentar al usuario los datos, así como de permitir la interacción con la aplicación. Típicamente, este elemento supone la interfaz gráfica de usuario. Por último, encontramos el controlador, que es el encargado de escuchar los eventos que tienen lugar sobre la aplicación (normalmente, interacción del usuario con la vista de la aplicación) e invocar los cambios pertinentes en el modelo y la vista.

Una secuencia típica de interacción de un usuario con una aplicación que sigue el patrón MVC sería la siguiente:

1.El usuario accede a la interfaz gráfica e interactúa con ella de alguna forma. Por ejemplo, pulsa un botón.
2.El controlador que escucha dicho evento recibe la notificación a través de algún manejador ("handler") o retorno de función ("callback"), y lo gestiona convenientemente.
3.El controlador modifica el modelo para ejecutar la acción solicitada por el usuario.
4.El controlador indica a la vista que el modelo ha cambiado, para que actualice su información en base a dichos cambios. La vista obtiene los nuevos datos del modelo y genera de nuevo la interfaz de usuario.
5.El ciclo se ha completado y la aplicación está lista para recibir nuevas interacciones.

A estas alturas, alguno de vosotros estará pensando "bla bla bla bla... ¿cuándo viene la acción?". Bien, pues como el movimiento se demuestra andando, andemos.

Manos a la obra

Lo primero que debemos saber es que en el patrón MVC seguido por Joomla, no existen ficheros de configuración que declaren explícitamente dónde se encuentra cada elemento del mismo. Joomla infiere el rol de cada fichero de código en base a una estructura de archivos y directorios como la que puede verse en la imagen adjunta.

En nuestro caso, vamos a crear un componente llamado "com_arroba" que deberá tener la siguiente estructura:

```
- [com_arroba]
- arroba.php
- controller.php
- [models]
- arroba.php
- [views]
- [arroba]
- view.html.php
- [tmpl]
- default.php
```

Para crear dicha estructura, usaremos los siguientes comandos:

```
ramiro@ubuntu:~$ cd /var/www/
joomla/components/
ramiro@ubuntu:/var/www/joomla/
components$ sudo mkdir com_arroba
[sudo] password for ramiro:
ramiro@ubuntu:/var/www/joomla/
components$ cd com_arroba/
ramiro@ubuntu:/var/www/joomla/
components/com_arroba$ sudo touch
arroba.php
ramiro@ubuntu:/var/www/joomla/
components/com_arroba$ sudo touch
controller.php
ramiro@ubuntu:/var/www/joomla/
components/com_arroba$ sudo mkdir
models
ramiro@ubuntu:/var/www/joomla/
components/com_arroba$ sudo mkdir
views
ramiro@ubuntu:/var/www/joomla/
components/com_arroba$ cd models/
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/models$
sudo touch arroba.php
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/models$ cd
../views/
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views$ sudo
mkdir arroba
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views$ cd
arroba/
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views/
arroba$ sudo touch view.html.php
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views/
arroba$ sudo mkdir tmpl
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views/
arroba$ cd tmpl/
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views/
arroba/tmpl$ sudo touch default.
php
ramiro@ubuntu:/var/www/joomla/
components/com_arroba/views/
arroba/tmpl$ cd ../../../../
ramiro@ubuntu:/var/www/joomla/
components$ sudo chown -R joomla.
www-data com_arroba/
```

```
ramiro@ubuntu:/var/www/joomla/
components$ tree com_arroba/
com_arroba/
|-- arroba.php
|-- controller.php
|-- models
|    `-- arroba.php
`-- views
   `-- arroba
     |-- tmpl
     |    `-- default.php
     `-- view.html.php

4 directories, 5 files
ramiro@ubuntu:/var/www/joomla/
components$
```

Bien, pues vamos a darle a la tecla. Empecemos por la parte más externa de la aplicación, lo que sería el punto de entrada del componente. Al recibir la petición "url/index.php?option=com_arroba", Joomla buscará un componente con dicho nombre, y ejecutará el script llamado "arroba.php" de la raíz de su estructura de directorios.

Este fichero contendrá el siguiente código:

```
<?php

defined('_JEXEC') or
die('Restricted access');
require_once(JPATH_COMPONENT.
DS.'controller.php');

if($controller = JRequest::
getWord('controller')){

  $path = JPATH_COMPONENT.
DS.'controllers'.
DS.$controller.'.php';

 if (file_exists($path)){
 require_once $path;
 }
 else{
 $controller = '';
 }

}

$classname    = 'ArrobaController
'.$controller;
$controller   = new $classname(
);

$controller->execute(JRequest::
getVar('display'));

$controller->redirect();

?>
```

La primera parte está encargada de comprobar si debe importarse un controlador específico, o si se utilizará el de por defecto. Así, genera el nombre de la clase del controlador en base a la nomenclatura de Joomla, que concatena el nombre del componente a la palabra "Controller"; concatenando todo ello a su vez al nombre específico del controlador, en caso de existir (variable "$controller"). En nuestro caso, supondremos que utilizaremos siempre el controlador por defecto, por lo que instanciaremos un "ArrobaController" del script "controller.php".

Bien, pues vamos a echar un ojo al código de dicho controlador...

```
<?php

defined('_JEXEC') or
die('Restricted access');
jimport('joomla.application.
component.controller');

class ArrobaController extends
JController
{

 function display()
 {
 parent::display();
 }

}

?>
```

Sencillo, ¿verdad? Realmente no hace nada, simplemente importa el comportamiento de los controladores de Joomla con la orden "jimport". Los posibles manejadores de eventos que queramos incluir en nuestra aplicación deberían ir aquí. Fijaos en el nombre de la clase: "ArrobaController", que es justo la que dijimos que queríamos instanciar.

Es la hora de meterle mano al modelo. Para ello, incluiremos en el fichero "arroba.php" del directorio "Models" el siguiente código:

```
<?php

defined('_JEXEC') or die();
jimport('joomla.application.
component.model');

class ArrobaModelArroba extends
JModel
{

 function getJson()
 {
 $data = file_get_
contents("http://localhost/
json");
 return $data;
 }

}

?>
```

Es importante, nuevamente, fijarse en el nombre de la clase: "ArrobaModelArroba". La nomenclatura en este caso sigue el esquema "nombre de componente + Model + nombre de modelo". Dado que en este caso el componente y el modelo tienen el mismo nombre, obtenemos "ArrobaModelArroba".

Como ya sabíamos, en el modelo realizamos el acceso a datos de la aplicación. Para

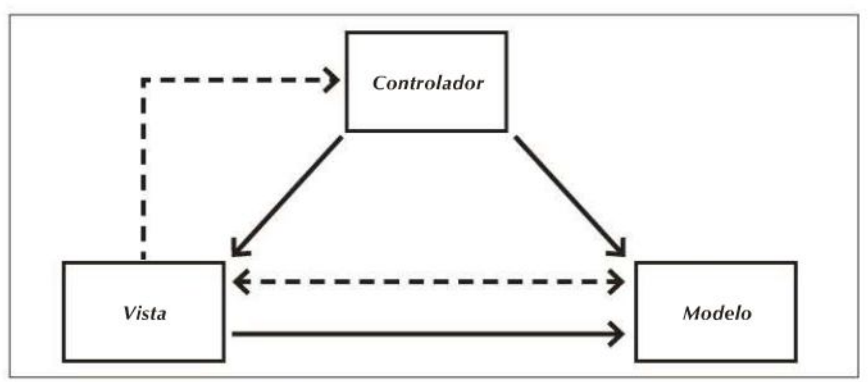
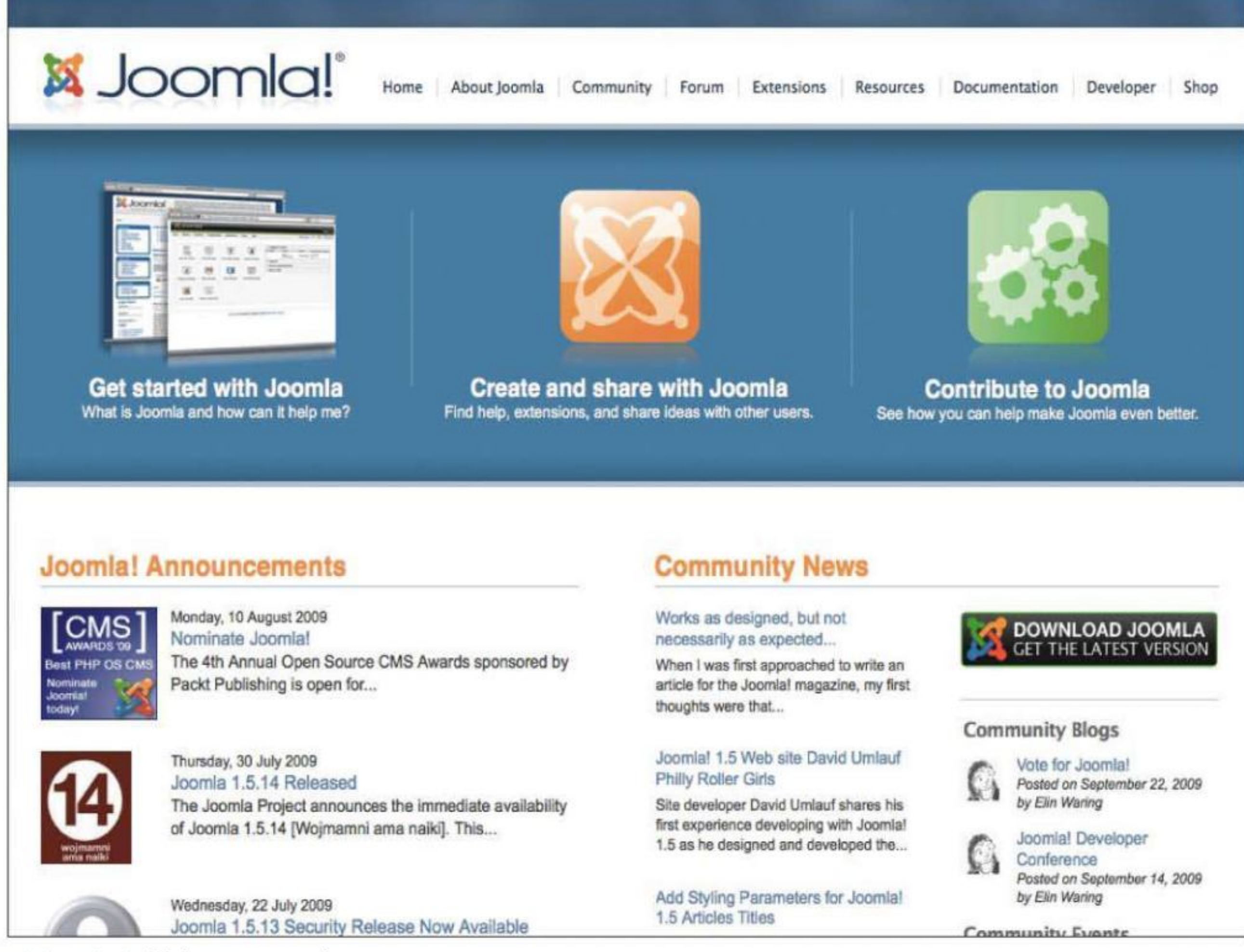


Diagrama del patrón Modelo-Vista-Controlador



Página principal del proyecto Joomla

que no sea tan aburrido como incluir un "echo" pegando algún texto, vamos a simular la llamada a un servicio web que, de alguna forma, nos devuelve un contenido en el formato ligero de intercambio JSON (JavaScript Object Notation).

Así de paso, hacemos que el ejemplo tenga algo más de vidilla, y no se parezca a los infinitos que existen en Internet.

Por supuesto, debemos crear un fichero en "/var/www/json" que contenga cierta información a leer después. En mi caso, introduje estos datos de ejemplo:

```
{"id":"Software v 0.1","description":"Es un programa precioso...","hits":"7"}
```

Así, la función "getJson" se encarga de llamar al servicio web (que bien podría ser uno real y, de hecho, el funcionamiento es idéntico) y devolver la información sin procesarla.

Últimos retoques

Ahora debemos hacer que la vista recupere la información del modelo. Para ello, el código del fichero "view.html.php" deberá ser como el siguiente:

```
<?php

defined('_JEXEC') or
die('Restricted access');
jimport('joomla.application.
component.view');

class ArrobaViewArroba extends
JView
{

  function display($tpl = null)
  {

  $model =& $this->getModel();

  $objeto_json = $model-
>getJson();
  $this->assignRef('mensaje',$obje
to_json);

  parent::display($tpl);

  }

}

?>
```

Nada nuevo, simplemente asignamos una referencia al objeto JSON recuperado, para que la plantilla de la vista pueda leer la información y formatearla adecuadamente. Así pues, sólo nos resta echar un ojo al código de dicha plantilla ("default.php"), que será el siguiente:

```
<?php
$obj = json_decode($this-
>mensaje);
echo "<p>Datos en bruto: ";
echo $this->mensaje;
echo '<p/>';
echo "<p>Identificador: ";
echo $obj->{'id'};
echo '</p>';
echo "<p>Descripción: ";
echo $obj->{'description'};
echo '</p>';
echo "<p>Número de visitas: ";
echo $obj->{'hits'};
echo '</p>';
?>
```

Realmente, en este caso se trata más de HTML que otra cosa... simplemente obtenemos los datos en bruto del JSON, los mostramos para verificar su corrección; y por últimos los formateamos para que queden un poco más monos.

Una vez picado todo el código, llega el momento de comprobar el funcionamiento. Para ello, introduciremos en nuestro navegador la URL "http://localhost/joomla/index.php?option=com_arroba" y comprobaremos si se muestra la información que debería:

```
Datos en bruto: {"id":"Software
v 0.1","description":"Es un
programa precioso...","hits":"7"}

Identificador: Software v 0.1

Descripción: Es un programa
precioso...

Número de visitas: 7
```

Si se muestra... ¡enhorabuena! Acabáis de crear vuestro primer componente para Joomla. Ya sois una pequeña parte más de la comunidad de desarrolladores de software libre para este fantástico CMS.

Terminando

Obviamente, el desarrollo de extensiones de Joomla no acaba aquí. Para empezar, nos dejamos en el tintero los módulos y los plugins, dos de los tipos de extensiones de Joomla. Además, y como habéis podido comprobar, hemos planteado uno de los ejemplos más simples que pueden imaginarse para generar código. A partir de aquí, podríamos continuar con acceso a base de datos, inclusión de funcionalidad AJAX, carga de servicios web externos e interacción con los mismos... las posibilidades son muy variadas.

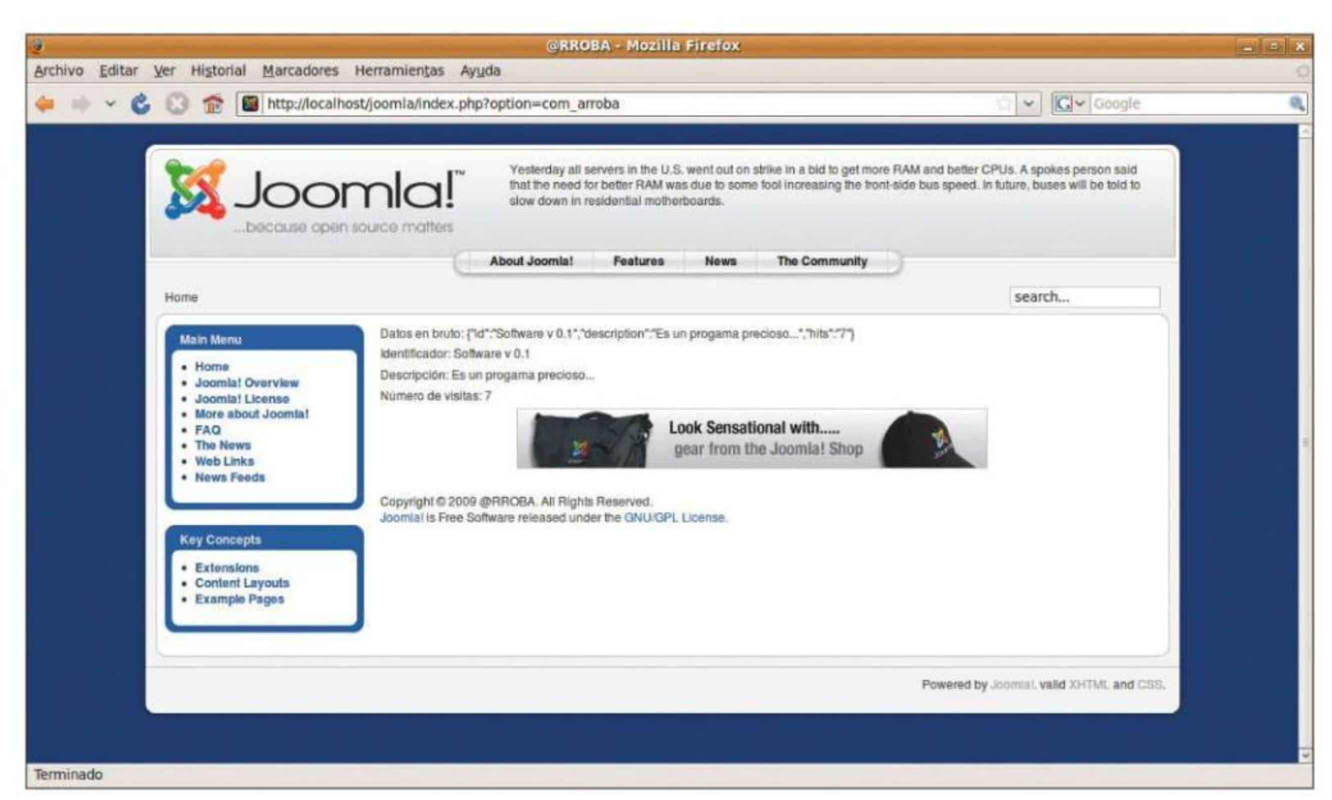
Por motivos prácticos, principalmente de espacio, resultaría imposible condensar en un único artículo la creación de un componente medianamente decente con funciones complejas, así como los conocimientos de PHP necesarios para llevar a cabo dicha tarea.

No obstante, y si habéis comprendido la estructura básica de los componentes en Joomla, y el funcionamiento del patrón de arquitectura Modelo Vista Controlador; estoy seguro de que no os resultará muy complicado dar los siguientes pasos, utilizando la abundante y fantástica documentación existente en Internet, así como los manuales de referencia del lenguaje de programación PHP.

Por supuesto, no os olvidéis de devolver a la comunidad los que obtuvisteis de ella: liberad el código de las extensiones que programéis. Quién sabe, quizá algún día alguien aprenda a programar nuevas extensiones mirando vuestro código...

¡Hasta la próxima!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/



Probando nuestro componente



Observer

Un patrón de diseño a observar

Observer es uno de los patrones de diseño más útiles y ampliamente utilizados que hay, siendo muy práctico tanto en una gran variedad de aplicaciones. Básicamente, el patrón Observer nos permite establecer una relación entre un objeto cuyo estado queremos observar y una serie de objetos (observadores) que deberán estar al tanto de los cambios en el primero.

Para los que desconozcan el término, los patrones de diseño son un concepto creado originalmente por el GOF (Gang Of Four, Erich Gamma, Richard Helm, Ralph Johnson y John Vlissides), cuya labor fue la de recopilar e identificar las interrelaciones de clases y colaboraciones entre objetos que acostumbramos a reutilizar, para simplificar el proceso de diseño y desarrollo de software.

Como parte de esta labor, crearon una serie de patrones de diseño, entendiéndose un patrón como "un conjunto de entidades (clases, relaciones, interfaces, etc.) que se interrelacionan entre sí y proporcionan una o varias soluciones para problemas habituales en el diseño de software".

En este artículo presentamos el patrón Observer, uno de los patrones de diseño más ampliamente utilizados.

El patrón Observer nos permite establecer una relación entre un objeto (publisher), del que queremos observar su estado (subject) o uno de sus estados, y una serie de objetos dependientes a los que identificamos como observadores (observers).

Con esta relación establecida, cuando el sujeto cambia de estado, todos los observadores dependientes son notificados y actualizados automáticamente.

La gracia de esto consiste en que el observador no depende de la implementación del sujeto y viceversa. El patrón Observer enfatiza tanto la encapsulación como el desacoplamiento de las clases que interactúan en él.

Es decir, el sujeto no tiene que saber ni cuántos observadores están al corriente de su estado ni de quiénes son estos; solamente deberá notificarles que ha cambiado. El sujeto no depende de la implementación de los observadores, y no habrá que modificarlo si varía uno de ellos.

El patrón Observer debería ser utilizado siempre que uno o más objetos (observadores) deban estar al corriente de los cambios que se produzcan en otro objeto (el sujeto). Este patrón se presenta con gran frecuencia en la vida real, siendo uno de los más interesantes, aunque no de los más sencillos de entender y aprender a utilizar.

A este patrón también se le denomina conoce como Publicación/Suscripción (Publish/Subscribe). El sujeto que desea exponer sus cambios de estado se publica (anuncia), y los observadores se suscriben para observar los cambios en él.

.NET y el patrón Observer

Como buena solución que es, el patrón Observer ha sido implementado en bastantes partes de la arquitectura de .NET Framework, apareciendo en muchos lugares de su librería de clases. Una de ellas es la implementación de las clases TraceListener (DefaultTraceListener, TextWriterTraceListener y EventLogTraceListener).

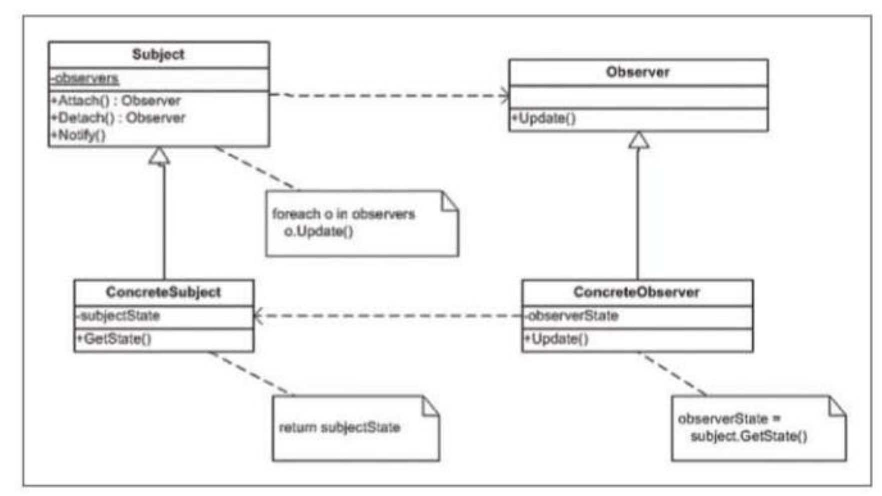
Anexando objetos de tipo TraceListener se habilita la recepción de notificaciones sobre diversos eventos.

```
TextWriterTraceListener Obser-
ver = newTextWriterTraceListe-
ner("c:\\bcndev.txt");
Trace.Listeners.Add(Observer);
Trace.AutoFlush = true;
Trace.Write("Hola Observer!");
```

¿Y cómo funciona?

En la figura 1 se presenta el esquema UML que expone el patrón y los participantes en el diseño del mismo:

En ella podemos identificar los diferentes elementos participantes del patrón ***(Fig.1)***.



(Fig.1) Esquema UML del patrón Observer.

LOS PATRONES DE DISEÑO SON UN CONCEPTO CREADO ORIGINALMENTE POR EL GOF (GANG OF FOUR, ERICH GAMMA, RICHARD HELM, RALPH JOHNSON Y JOHN VLISSIDES), CUYA LABOR FUE LA DE RECOPILAR E IDENTIFICAR LAS INTERRELACIONES DE CLASES Y COLABORACIONES ENTRE OBJETOS QUE ACOSTUMBRAMOS A REUTILIZAR, PARA SIMPLIFICAR EL PROCESO DE DISEÑO Y DESARROLLO DE SOFTWARE.

• **Subject** representa al sujeto o elemento observado de forma abstracta (superclase).

- Proporciona una forma de asignar y desasignar observadores.

- Mantiene una lista de los observadores.

- Notifica a los observadores cuando acontece un cambio.

• **ConcreteSubject** Representa al sujeto concreto que es observado.

- Contiene el elemento de interés (estado del sujeto) para los observadores.

- Envía una notificación a sus observadores cuando cambia su estado. Ello lo realiza invocando al método **Notify**() de su superclase (**Subject**).

• **Observer** Representa al observador de forma abstracta (superclase).

- Proporciona una interfaz de actualización para todos los observadores concretos (**ConcreteObserver**), mediante la que éstos pueden recibir una notificación de la actualización del sujeto.

• **ConcreteObserver** representa a un observador concreto.

- Mantiene una referencia al **ConcreteSubject.**

- Puede almacenar información sobre el estado del sujeto que está siendo observado.

- Implementa el método **Update**(), redefiniendo el método de la clase base **Observer**. Este método mantiene el estado consistente con el del **ConcreteSubject**, invocando a la función **getState()** del **ConcreteSubject** para actualizar la información sobre el estado de éste.

Como muestra, un botón...

Todo esto puede parecer complejo, pero no lo es una vez se entienden los conceptos y se han aplicado. Y siendo la aplicación práctica la mejor forma de entenderlo, vamos a presentar una aplicación del patrón, que vamos a realizar de forma fundamentalmente estructural, siguiendo el diagrama UML propuesto por el GOF.

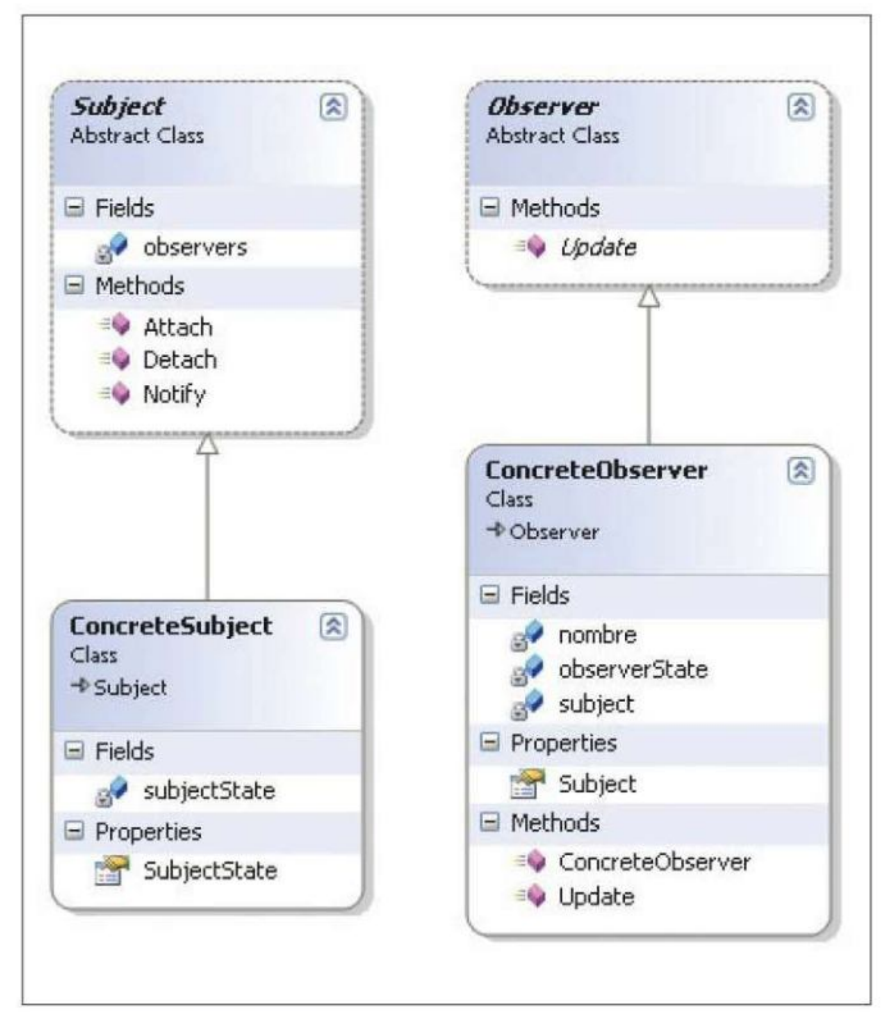
Vamos a crear, para los sujetos a observar, una clase Subject y una clase derivada ConcreteSubject. Por lo que respecta a los observadores, crearemos una clase Observer y una clase ConcreteObserver que deriva de la anterior.

En aras de la sencillez y de mostrar un ejemplo del patrón "sin más" se ha implementado el siguiente diagrama de clases en una aplicación de consola ***(Fig.2)***.

Esta es la representación más "pura" del patrón Observer, en la cual se pueden ver representadas en las clases y en el código las interactuaciones de los diferentes conceptos propuestos por este patrón.

Cabe destacar que la implementación suele variar y hay muchas mejores implementaciones que ésta, cuya ventaja es que es la que expone más claramente el patrón, haciéndolo más comprensible.

Como podemos ver en el código, además de la definición de las entidades participantes del patrón, creamos un sujeto concreto que llamamos CS:



(Fig.2) Diagrama clases observer

```
ConcreteSubject CS = new Concre-
teSubject();
```

Luego generamos cuatro observadores concretos a la vez que los vamos asignando al sujeto:

```
CS.Attach(new ConcreteObserver(CS,
"CO_A"));
CS.Attach(new ConcreteObserver(CS,
"CO_B"));
CS.Attach(new ConcreteObserver(CS,
"CO_C"));
CS.Attach(new ConcreteObserver(CS,
"CO_D"));
```

Por último, cambiamos el estado del sujeto y lanzamos la notificación del mismo:

```
// Cambiamos el sujeto
CS.SubjectState = "ABC";

// Y notificamos
CS.Notify();
```

Ello invocará el método **Update()** de los observadores concretos e imprimirá un mensaje en la consola.

El código de la aplicación de ejemplo se presenta en el fuente 1.

```
// Patron Observer
// Ejemplo estructural
namespace JL.GangOfFour.
ObserverPattern
{
  class MainApp
  {
  static void Main()
  {
```

>>> EJEMPLOS DE LA APLICACIÓN DEL PATRÓN OBSERVER

- **Esperar a que se produzca algún evento, una acción del usuario o una respuesta de un servicio para, por ejemplo, actualizar la interfaz de usuario, la base de datos o ambos.**
- **Esperar a que se produzca un cambio en el valor de una propiedad de un objeto.**
- **Esperar a que se produzca el cambio de un valor en el almacén de datos (*trigger*).**

```
  // Configuramos el patrón Observer
  ConcreteSubject CS = new
ConcreteSubject();

  CS.Attach(new ConcreteObserver(CS,
"CO_A"));
  CS.Attach(new ConcreteObserver(CS,
"CO_B"));
  CS.Attach(new ConcreteObserver(CS,
"CO_C"));
  CS.Attach(new ConcreteObserver(CS,
"CO_D"));

  // Cambiamos el Sujeto(Subject)
que estan observando los
Observadores(Observers)
  CS.SubjectState = "ABC";

  // Y notificamos
  CS.Notify();

  // Esperamos al usuario
  Console.Read();
  }
  }
```

Fuente 1. Código de la aplicación de ejemplo

A continuación, exponemos brevemente la implementación de las clases de sujetos y observadores. El sujeto (**Subject**) está programado en el fuente 2, en el que definimos la clase abstracta Subject, en la cual tenemos implementados los métodos **Attach()** y **Detach()** para asignar o desasignar observadores y el método **Notify()**, que nos servirá para invocar el método **Update()** de los objetos **Observer** que tengamos asignados a este Subject.

```
  // Definición de los sujetos
(Subject y ConcreteSubject)
  // Subject
  abstract class Subject
  {
       private ArrayList observers
= new ArrayList();

       public void Attach(Observer
observer)
       {
       observers.Add(observer);
       }

       public void Detach(Observer
observer)
       {
       observers.Remove(observer);
       }

       public void Notify()
       {
       foreach (Observer o in
observers)
       {
       o.Update();
       }
  }
}
```

Fuente 2. Sujetos.cs

Luego tenemos la implementación de ConcreteSubject (fuente 3), clase que hereda de Subject y en este caso solo aporta el estado, sobre cuyos cambios los objetos Observer quieren estar al tanto.

```
  // ConcreteSubject
  class ConcreteSubject : Subject
  {
       private string subjectState;

  public string SubjectState
```

COMO HEMOS VISTO AQUÍ, OBSERVER ES UN PATRÓN MUY ÚTIL. ESTE PATRÓN SE UTILIZA AMPLIAMENTE EN ARQUITECTURAS DE SOFTWARE DE TODO TIPO.

```
  {
        get { return subjectState; }
        set { subjectState = value;
}
        }
  }
```

Fuente 3. ConcreteSubject.cs

Para los observadores, tenemos el fichero Observadores.cs (fuente 4), en el que definimos la clase abstracta Observer, con un único método abstracto, Update(), a implementar obligatoriamente en las clases derivadas de ella.

Este método es el que invocaba el método Notify() de la clase Subject.

```
// Observer
  abstract class Observer
  {
  public abstract void Update();
}
```

Fuente 4. Observer.cs

La clase ConcreteObserver (fuente 5) solamente implementa el método Update(), que no es más que la obtención del ConcreteSubject asignado en su creación, y realiza una impresión de su valor actual y del nombre del objeto.

```
  // ConcreteObserver
  class ConcreteObserver : Observer
  {
        private string nombre;
        private string
observerState;
        private ConcreteSubject
subject;

        public ConcreteObserver(
        ConcreteSubject subject,
string nombre)
  {
        this.subject = subject;
        this.nombre = nombre;
  }

        public override void
Update()
  {
        observerState = subject.
SubjectState;
        Console.WriteLine("El nuevo
estado del Observer {0} es {1}",
        nombre, observerState);
  }

        public ConcreteSubject
Subject
  {
        get { return subject; }
        set { subject = value; }
  }
}
```

Fuente 5. ConcreteObserver.cs

Si ejecutamos la aplicación, ésta en primer lugar crea una instancia de ConcreteSubject y luego crea los ConcreteObserver (de nombre CO_A, CO_B, CO_C, CO_D) y les realiza un Attach() al sujeto, con lo que estos observadores quedan suscritos.

Posteriormente modificamos el valor del estado del sujeto y llamamos a su método Notify(). Éste invoca al método de la clase base abstracta de la cual hereda (Subject) y a los métodos Update() de todos los ConcreteObserver.

El resultado es que cada uno de ellos obtiene el estado del sujeto y realiza una impresión en la consola de dicho estado.

CABE DESTACAR QUE LA IMPLEMENTACIÓN SUELE VARIAR Y HAY MUCHAS MEJORES IMPLEMENTACIONES QUE ÉSTA, CUYA VENTAJA ES QUE ES LA QUE EXPONE MÁS CLARAMENTE EL PATRÓN, HACIÉNDOLO MÁS COMPRENSIBLE.

Acerca de la implementación

Cabe destacar que existen muchas formas de aplicar este patrón; en lugar de herencia podemos utilizar interfaces o bien delegación, en aras de un mayor desacoplamiento, u otras técnicas para mejorar la gestión del estado.

También seguramente habréis pensado que esta versión sirve solamente para un estado por objeto o clase (observador y sujeto)...

Aquí ya entramos en las diferentes posibles implementaciones del patrón y su aplicación técnica en función del lenguaje utilizado, tema sin duda para otro artículo. En este artículo nos hemos acercado al concepto del patrón Observer y hemos realizado una implementación muy estricta, clara y concisa de su diseño original.

Conclusiones

Como hemos visto aquí, Observer es un patrón muy útil. Este patrón se utiliza ampliamente en arquitecturas de software de todo tipo. De hecho, junto a Singleton es uno de los dos más utilizados; claro está, sin dejar de lado a otros interesantes patrones, como Factory, Strategy, Façade, Template, Adapter, etc., que son la base de los patrones de diseño en el software.

José Luis Latorre es arquitecto de software especializado en tecnología RIA e UX (WPF, Silverlight, Surface), MCTS y MVP de Microsoft. Es el fundador y actual coordinador de BcnDev, la asociación de desarrolladores .Net de Barcelona, www.bcndev.net. Es colaborador de IN2, http://www.in2.es y de BrainSiders, http://www.brainsiders.com, especializada en desarrollos web de última generación.

QUE EXISTEN MUCHAS FORMAS DE APLICAR ESTE PATRÓN; EN LUGAR DE HERENCIA PODEMOS UTILIZAR INTERFACES O BIEN DELEGACIÓN, EN ARAS DE UN MAYOR DESACOPLAMIENTO, U OTRAS TÉCNICAS PARA MEJORAR LA GESTIÓN DEL ESTADO.



FRIKI GADGET

LO MAGICO DE UN DíA DE COMPRAS



Aventuras de un geek en el país del Sol Naciente



Héctor García, conocido en Internet como Kirai, saltó a la fama por su blog -www.kirainet.com- escrito desde Japón donde lleva ya viviendo casi cinco años. Hace poco esta bitácora digital dio el salto al papel y ahora se acaba de presentar la tercera edición de este libro que lleva vendidos más de 10.000 ejemplares.

A este alicantino de 28 años, Japón le sedujo ya a temprana edad. "Finales de los años ochenta era la época de oro japonesa: el mundo estaba lleno de walkmans, las series de la tele también eran japonesas,... la tecnología venía de Japón", recuerda Héctor García, alias Kirai. "De pequeño ya empezaba a sentir fascinación por la tecnología japonesa, quería aprender a construir ordenadores". Después de estudiar Ingeniería Informática en Alicante y hacer una breve estancia en el CERN (Suiza), se marchó a Japón porque le seguía fascinando. Y cuando llegó, lo que halló supero todas sus expectativas: "Japón es lo más parecido a visitar una civilización extraterrestre tecnológicamente avanzada", indica García. "Me encontré como si estuviera en otro planeta y tuve que comenzar a explorar". Y así empezó a recoger en un blog sus experiencias y las curiosidades que veía y conocía, creando 'Kirai, un geek en Japón' en enero de 2003. Poco a poco ha ido llenando páginas de esta bitácora, plasmando y compartiendo allí los resultados de esta navegación por tierras niponas. El blog, que cuenta con más de 3.700 posts de unas 70 categorías, recibe más de 50.000 visitas al día de internautas de todo el mundo que han dejado hasta ahora 121.953 comentarios. Orgulloso de que su blog se haya convertido en una de las bitácoras de referencia para quienes están interesados en el país del Sol Naciente, Kirai reconoce que tanta información (blogs, videos en YouTube, etc) en la Red tiene una parte un poco negativa. "Creo que se está spoileando Japón, -como pasa con los trailers de las películas que casi te cuentan el final-, desvelando las peculiaridades con las que luego el viajero se va a encontrar", lamenta. "En cualquier caso, sigue siendo sorprendente aún para la gente que va ahora por muy informada que esté".

Tecnología global

Aunque fascinado por la capacidad tecnológica de los japoneses, García no duda en afirmar que la época dorada de la tecnología nipona ya ha pasado. "Ahora las factorías están fuera del país (China, Corea del Sur) aunque en Japón se sigue manteniendo el diseño", indica. "Algo ha pasado: antes el walkman era japonés y ahora el iPod es americano. Los japoneses siguen triunfando en los videojuegos pero en otras áreas están como atascados". Una de las grandes apuestas tecno-

>>> VIDA DE UN OTAKU

Otaku es una palabra japonesa que se ha internacionalizado y se usa para referirse a gente obsesiva con sus hobbies, sobre todo relacionados con el anime y el manga.

El origen de la palabra otaku

La palabra otaku tiene un origen curioso. En japonés es un término que se utiliza para referirse a la casa de otra persona, pero también es un pronombre de segunda persona honorífico poco común, algo así como el "usted" castellano. Parece ser que la comunidad friki japonesa utilizaba mucho el pronombre otaku para referirse a sus iguales cuando realmente no es necesario utilizar un pronombre tan formal. Poco a poco, gente de fuera de las comunidades frikis se dio cuenta de este fenómeno y comenzó a utilizar la palabra otaku para referirse a los frikis. Durante los años noventa se convirtió en una palabra de uso común en Japón y a finales de siglo se comenzó a extender por todo el mundo, no solo como una palabra sino como un movimiento cultural.

¿Qué es un otaku?

Para un japonés, un otaku es aquel que pasa mucho tiempo libre encerrado en casa dedicándose a cultivar aficiones de lo más diversas. Los otakus más abundantes en Japón son los aficionados a leer manga, a los videojuegos, al anime o, simplemente, enganchados a Internet. La palabra otaku, en principio, tenía un sentido bastante despectivo en los años noventa, dando a entender que un otaku no tenía vida propia más allá de Internet o de sus cómics favoritos. Pero la palabra se exportó al extranjero y tomó el sentido de 'aficionado a la cultura japonesa' y, sobre todo, friki del anime y el manga. El significado que tomó en el extranjero retornó a Japón dándole un sentido algo más positivo y, actualmente, la mayoría de la gente simplemente lo usa para bromear con los colegas en plan 'eres un otaku de la música de los 70', 'eres un otaku de Ghibli', 'otaku de Gundam', 'otaku de ordenadores', etc.

Tipos de otakus más definidos y populares en Japón

• **Manga otaku:** No solo leen manga (algo que hacen la mayoría de japoneses sin ser otakus) sino que coleccionan todo tipo de material relacionado con sus series favoritas.

• **Anime otaku:** Parecidos a los anteriores pero se centran más en coleccionar DVD de sus series favoritas.

• **Figure otaku:** Coleccionan figuritas de series. Hay todo un mundo de figure otakus, tienen sus propias convenciones internacionales, tiendas e incluso centros comerciales enteros de figuritas en Akihabara.

• **Pasokon otaku:** Obsesionados con los ordenadores, tienen servidores en sus casas para montar comunidades de otakus, siempre están a la última, comprando y vendiendo en tiendas de Akihabara. Muchos de ellos también son aficionados a construir robots y a hacer montajes electrónicos.

• **Wota:** Otakus de idols. Son fans de las características idols, ya sean de tipo gravure (chicas que posan en bikini) o cantantes de las cuales coleccionan su música, DVD y libros de fotos.

• **Gemu otaku:** Otakus de los videojuegos. Tienen todas las videoconsolas del mercado y suelen estar centrados en juegos de rol de los cuales se compran todas las guías disponibles en las librerías. Hay todo un mercado de libros de videojuegos en Japón dirigido exclusivamente a ellos.

• **Densha otaku:** Otakus de los trenes que coleccionan figuritas de todos los trenes de Japón y están a la última comprando revistas en las que informan de los últimos modelos de locomotoras y vagones.

(Extracto del capítulo 7 de 'Un geek en Japón' de Héctor García)





lógicas de Japón a finales del s.XX fue la domótica, con la incorporación de numerosas instalaciones orientadas a conseguir el hogar automatizado, la casa del futuro. "La casa en la que yo vivo en Tokio fue construida a finales de los 80 y cuenta con un gran número de botoncitos distribuidos por toda ella con funciones de lo más variopintas. Tras casi tres años de alquiler aún no sé para qué sirven todos. El más curioso es uno que, desde la cocina, me permite saber la temperatura del agua de la bañera y poderla regular". Según comenta García, las casas actuales ya no tienen incluida toda esta tecnología. Y es que desde fuera de Japón tendemos a considerar que allí siempre está a la última en tecnología, pero esta etiqueta se va borrando porque los grandes lanzamientos tecnológicos son globales y en semanas o meses están disponibles en otros países. "Primero se lanza en Japón, poco después en Estados Unidos y a las pocas semanas, en el resto de mundo. En cambio con la Wii pasó algo inaudito y se lanzó primero en Estados unidos que en Japón", recuerda.

Fenómeno móvil

Un área en la que despunta por encima de todos los países pero que resulta compleja de exportar o replicar es la de los móviles. "Allí Nokia no triunfó porque sus teléfonos eran considerados demasiado obsoletos para el mercado japonés". En cambio, los fabricantes nipones tampoco se han planteado exportar sus avanzadísimos teléfonos puesto que no han sabido como adaptarlos o sería tan costoso que no resulta rentable. "Los teléfonos japoneses están muy adaptados al idioma y a otras características muy particulares japonesas. Aunque ahora, los expertos nipones hablan de cómo salir de la crisis y se fijan en el caso paradigmático del iPhone que ha invadido el mundo". Una de las particularidades más destacadas de los usuarios de teléfonos móviles japoneses es que éstos no envían SMS. "Desde el año 1999 utilizan el correo electrónico en el móvil. Es decir, llevan 10 años de ventaja respecto

al resto del mundo. Por ello no podían exportar sus móviles sin tener que hacer cambios costosos". Además en Japón prácticamente todo el mundo tiene tarifa plana de acceso a Internet desde el móvil por lo que éste se ha convertido en el dispositivo de acceso a Red por encima del PC. Según relata García, el ordenador está pasando a ser la herramienta de trabajo, el móvil es para acceder a Internet y la TV junto con la consola se está convirtiendo en una estación multimedia. Para Kirai, otra de las cosas tecnológicamente más sorprendente es su capacidad para mantener lo antiguo integrándolo con lo nuevo, o al contrario, introduciendo adelantos y novedades sin despreciar lo antiguo. "Por ejemplo, siguen teniendo trenes de vapor que van a carbón funcionando al lado de los trenes bala".



Y un mito que también está despareciendo es que sea más barata la tecnología. Según Kirai, es más fácil encontrar ordenadores baratos en Media Markt que en Akihabara. Y "Las tarjetas de memoria SD me las compro en España porque están mejor de precio. En cambio las cámaras fotográficas y complementos como lentes son algunos de los productos que aún se puede encontrar bastante más baratos. Sobre todo si es una cámara cara, te puedes ahorrar casi el viaje", apunta. Asimismo destaca la rapidez para crear aplicaciones que permitan el uso masivo de una nueva tecnología. Éste sería el caso de Internet en los móviles, se lleva utilizando desde hace muchos años. También se utiliza de manera habitual el móvil como monedero electrónico para micropagos (metro, por ejemplo).

Twitter a la japonesa

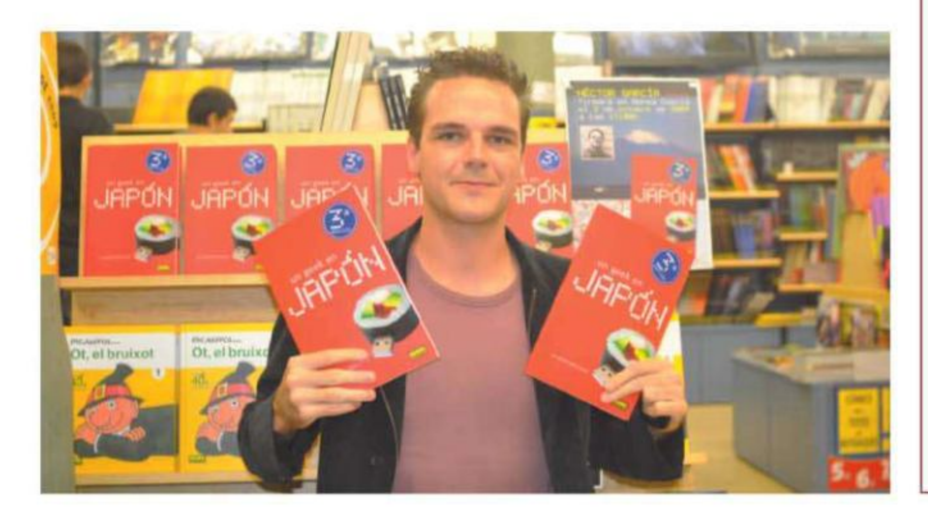
Tras pasar por Technorati y por la experiencia de montar su propia empresa, Mirai, ahora Héctor García trabaja para Twitter en Japón. Usuario de este servicio de microblogging desde el principio, ha colaborado en la adaptación del mismo al japonés. "Ahora Twitter se puede usar en japonés además de en inglés. Si en España hubiera una empresa interesada se podría traer en castellano". De esta manera se pretende aumentar el número de usuarios, rompiendo limitación impuesta por la barrera idiomática. "Al estar disponible en japonés, Twitter en está llegando a más gente, saliendo de los círculos más frikis. Además en los nuevos teléfonos móviles se va a incorporar una serie de accesos directos en los menús para que sea más sencillo y directo usar el servicio, con solo tres pulsaciones". Con esta estrategia se prevé todo un boom del microblogging. "De hecho Tokio es la ciudad en la que más se twittea y Japón es el segundo país en número de usuarios después de Estados Unidos". Según explica Héctor García, las empresas niponas también han empezado a interesarse por el servicio y lo quieren usar para vender o anunciar sus productos. Desde estas cuentas corporativas, una empresa puede comunicar a sus seguidores la oferta de una pantalla plana con un 10% de descuento a la venta durante los siguientes 10 minutos, por ejemplo.

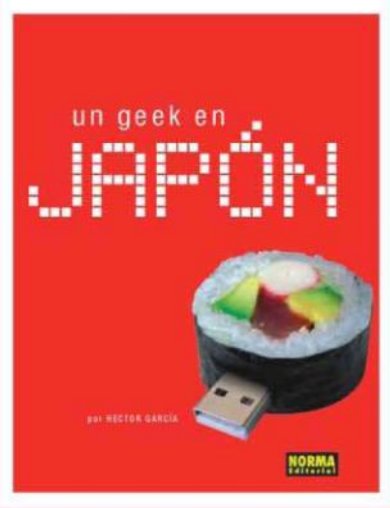
Gadgets increíbles

Para los más geeks y frikis, Japón es también el país de procedencia de un sinnúmero de gadgets a cual más sorprenden e incluso a veces inútil o inverosímil. Recientemente Kirai recogía en su web un post dando a conocer la almohada que te abraza. ¿Por qué dise-

>>> 'UN GEEK EN JAPÓN', EL LIBRO

¿Te fascina la cultura japonesa? ¿Sueñas con viajar a Japón? Héctor García, alias Kirai, también soñaba con viajar a Japón y este sueño se hizo realidad porque actualmente vive y trabaja en el país del Sol Naciente. El libro explica algunas de las claves culturales más importantes para entender el pensamiento japonés, la filosofía y religión que impera en el país, el estado actual de la sociedad, las tribus urbanas que conviven en las grandes metrópolis japonesas, la cultura pop, el manga y anime, la música y el cine. El libro termina con un par de capítulos con algunos de los lugares a visitar favoritos del autor. ¿Quieres conocer mejor la cultura y sociedad japonesa? ¿Te fascina el J-Pop, el manga, el anime? ¿Vas a viajar a Japón dentro de poco? De todo esto se habla en el libro del que el autor y la editorial ofrece un capítulo para descargar como muestra. http://www.kirainet.com/capitulo-7-de-un-geek-en-japon-en-pdf/





>>> AKIHABARA

Akihabara es el barrio de tiendas de electrónica más grande del mundo. Es la meca de los geeks/frikis/otakus/nerds de todo el mundo. Centenares de tiendas y centros comerciales especializados en gadgets, componentes electrónicos, anime, figuritas, videojuegos, robots, manga, cosplay... Está a dos paradas de la estación de Tokio, y desde hace sesenta años se ha conocido el apodo de Ciudad Eléctrica ('Electric town'). En los años 50 se vendían radios, en los años 60 y 70 televisiones, lavadoras y neveras, en los 80 y 90 fue el boom de los ordenadores personas y los videojuegos y desde hace poco la cultura del manganime y otaku en general está conquistando Akihabara. El barrio es también un manantial de movimientos sub-culturales japoneses como por ejemplo el cosplay, meido kissas, akiba-kei (grupo/tendencia social de todo aquello relacionado con Akihabara) y muchos otros. Lo que más me gusta de Akihabara es la variedad de tiendas y la especialización cada una de estas. Puedes encontrar desde tiendas de artilugios y juguetes sexuales hasta tiendas que sólo venden transistores o condensadores. Si no te quieres complicar yendo de tiendecita en tiendecita, también tienes grandes centros comerciales como el Yodobashi (el más grande el mundo). Pequeñas tiendas y centros comerciales, nuevos gadgets y cámaras que todavía no se venden fuera de Japón, videojuegos y trastos que nunca se venderán en el extranjero, tiendas de ordenadores y videojuegos de segunda mano, todo mezclado para atraer la atención de todo tipo de frikis. Las primeras veces que vine a Akihabara no me enteré de la película. Para empezar a ver de verdad la esencia del barrio te tienes que adentrar por las callejuelas, meterte en bajos o subir por escaleras escondidas en edificios que parecen deshabitados pero están llenos de tiendas 'secretas' (normalmente de trastos de segunda mano). En las tiendas pequeñas puedes incluso regatear.

Variedad comercial

Algunas de las diferentes tiendas que podemos encontrar en Akihabara son:

• **Centros comerciales:** alrededor de la estación se acumulan los más grandes: LAOX, Ishimaru, Yodobashi, Sato Musen. En ellos encontrarás: TVs, cameras, videogames, laptops, lavadoras etc. Te harán un 5% (Tax free) de descuento si enseñas el pasaporte. Ishimaru, LAOX y Yodobashi son los tres centros comerciales más grandes del barrio.

• **Tiendas de ordenadores:** en los años noventa el mayor negocio de Akihabara eran los ordenadores, ahora mismo no es un sector tan importante pero todavía hay tiendas especializadas. Las más famosas son Tsukumo y Softmap, las podéis encontrar cruzando la avenida principal. También en la misma zona hay montones de tiendas de ordenadores y componentes en las que los precios suelen ser algo más bajos que en Tsukumo o Softmap.

• **Hobby stores:** son tiendas especializadas en merchandising y figuritas de series de anime, películas, series o videojuegos. Si quieres comprar una figurita de tu serie favorita Kotobukiya y Asobit son las dos tiendas con más variedad, están justo al lado de la estación.



• **Manga y anime:** hay edificios enteros llenos de manga y DVDs de anime, el sueño de todo otaku. Las tiendas más importantes son Mandarake, Animate y Japanimation que están subiendo la avenida principal a mano derecha.

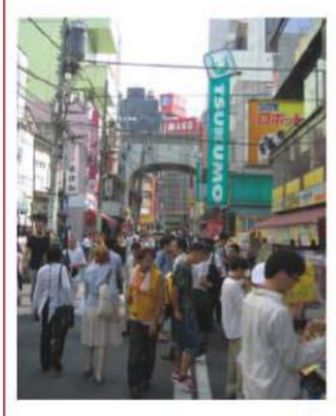
• **Videojuegos:** hay muchas tiendas de juegos donde no solo puedes comprar novedades, si vas a la segunda o tercera planta (casi siempre hay más de una planta en las tiendas de Akihabara, aunque no lo parezca a simple vista) encontrarás juegos descatalogados. Un sitio muy recomendable es Superpotato, donde tienen juegos incluso de MSX, Superfamicom, Virtual Boy…

• **Electrónica:** hay muchas tiendas de electrónica concentradas junto a la estación debajo de las vías del tren, el conjunto de todas estas tiendas forma lo que la gente de Akihabara conoce como el 'Radio Center'. Es uno de mis lugares favoritos, verás a gente seleccionando cuidadosamente transistores o comprando piernas/brazos para montar robot humanoides. Me recuerda al mercado de Alita (Gunnm). El Radio Center es una especie de mercadillo de micro-tiendas de componentes electrónicos, encajonadas en pasillos bajo las vías del tren.

• **Meido Kissas:** son cafeterías en las que te atienden chicas vestidas de criada. Cuando entras en una Meido Kissa, varias chicas te dan la bienvenida diciendo: "Bienvenido, honorable hombre de la casa" y te hacen una reverencia. Hay muchas Meido Kissas últimamente y están anunciadas en cualquier esquina. También puedes optar por aceptar la invitación de alguna Meido que hace promoción en la calle.

Un consejo final, si sólo tienes un día para visitar Akihabara es que vayas a los centros comerciales a comprar lo que tengas en mente, el servicio y los precios son bastante buenos. Luego dedica el resto del tiempo a visitar los lugares en los que estés más interesado: si te interesa el manganime ve directamente a Animate o Mandarake, si te gustan las figuritas y merchandising ves directamente a Asobit o Kotobukiya. Cada tienda es enorme y puedes pasar varias horas dentro de ellas, así que si tienes poco tiempo selecciona bien las tiendas a visitar.

Por Kirai (http://www.kirainet.com/akihabara)







ñan los japoneses este tipo de cosas frikis? "Lo hacen porque son frikis aunque ellos cuando lo crean no lo consideran frikadas sino cosas útiles", afirma. "Así en el caso de la almohada con brazo, el ingeniero que la ha creado podría explicar que la diseñado con esa curvas para que sea más fácil de usar, qué mejoras puede aportar, etc". Y en este tema, el que más patentes tiene es Dr. Nakamatsu, quien ha diseñado una zapatillas con muelles "y explica muy serio en los anuncios las principales ventajas de usarlas: por ejemplo, llegar a tiempo a las reuniones, etc. Creo que se han puesto de moda en San Francisco..." Otra de cosas más frikis que Kirai recuerda con sorpresa es un para plátanos. "Lo reseñé en el blog como algo inútil y al poco tiempo una compañera del trabajo lo estaba usando. Ahora creo que ya está a la venta en España. A veces ves cosas curiosas de las que te ríes pero luego triunfan porque a la gente les gustan".

Salto al papel

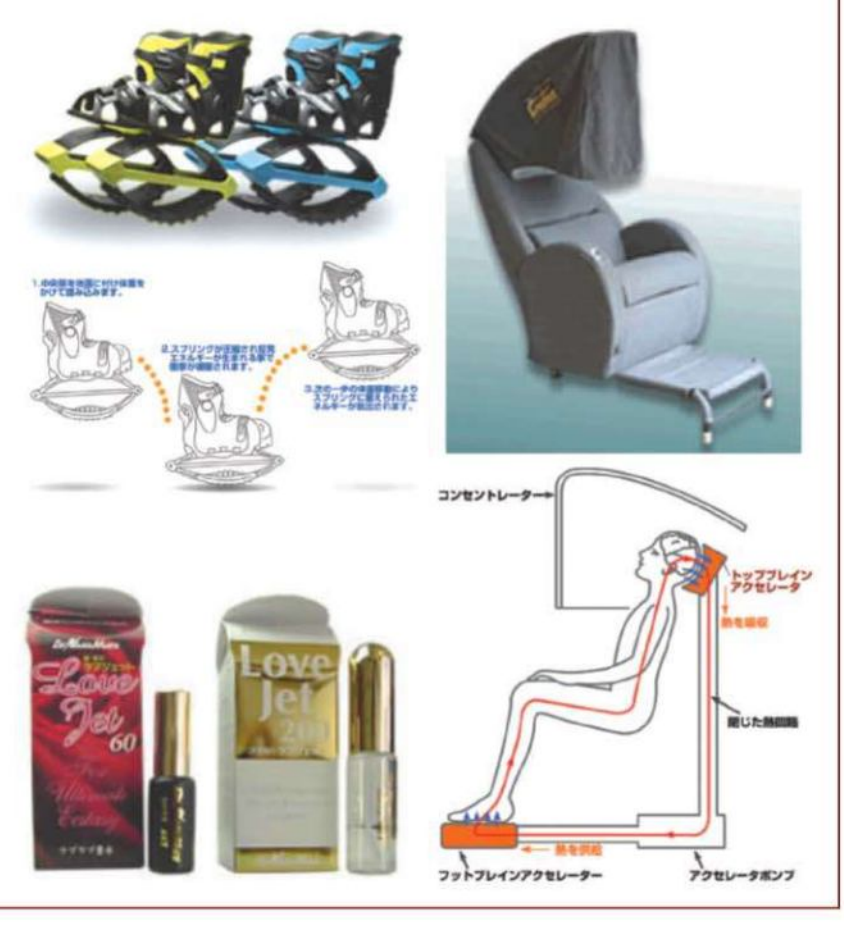
Con el paso del tiempo y el aumento de posts y de visitas, Héctor García se dio cuenta de que había plasmado muchas vivencias e inquietudes en el blog pero que le quedaban muchas otras en el cuaderno de apuntes. Entonces juzgó interesante escribir un libro acerca de todo lo que había aprendido sobre el país del Sol Naciente. En el libro 'Un geek en Japón', editado por Norma Editorial, Kirai cuenta lo que ha aprendido viviendo en este país durante los últimos años, desde la forma de ser de la gente hasta sus lugares favoritos en Tokio. "Es una recopilación y ampliación de los mejores contenidos de www.kirainet.com, que ha habido que adaptar porque no es lo mismo el tipo de lenguaje que se emplea en un medio que en otro o porque en el blog se usan los enlaces para dar más información mientras que en el libro toca explicarlo". Al final se convirtió en un trabajo de más de tres años. "Sin duda, a la que más ilusión le ha hecho el libro es a mi madre". Recientemente el autor ha estado de visita en Madrid y Barcelona, presentando en Casa Asia, en el marco de las jornadas Asian Geek, la tercera edición del libro del que se han vendido más de 10.000 ejemplares. "Ha tenido más éxito del que esperaba y me he dado cuenta que con el libro he conseguido lectores para el blog y viceversa. Los lectores del libro son bastante diferentes. Como anécdota destacar que el verano pasado me encontré por las calles de Shibuya con un grupo de abuelas de Segovia que me reconocieron y me pararon para que les firmara el libro". A aquéllos que se piensen si lanzarse a una aventura parecida, Kirai no duda en animarlos. "A todo el mundo le digo que salga de España porque da otra perspectiva y tener al menos dos perspectivas es bueno". Y si el destino elegido es Japón, "nadie se a arrepentir. Viajar es bueno pero la experiencia vivir fuera es diferente y si es en un sitio como Japón es ya para fliparlo", asegura García, emocionado y reconoce que esta experiencia le ha cambiado. "Soy una persona totalmente diferente de la que llegó a Japón hace cinco años, ni mejor ni peor, diferente".

>>> DOCTOR NAKAMATSU



Hace unos días descubrí a el doctor Nakamatsu, no se porqué nunca había oído hablar de él. Es un inventor japonés que tiene 81 años y tiene ya más de 3.000 patentes bajo el brazo, más del triple de las que consiguió Thomas Edison en vida. Muchas de sus primeras patentes fueron licenciadas a IBM y dieron lugar a la creación de los disquetes (floppy). IBM lo reconoce como el inventor del floppy. También tiene un montón de patentes relacionadas con la creación de los primeros relojes digitales y sintetizadores musical, Casio lo reconoce como el inventor del reloj digital. Además ha escrito algo más de 80 libros y dice que antes de morir va a conseguir llegar a más de 7.000 patentes-invenciones. Entre todas esas más de 3.000 invenciones tiene algunas de lo más curiosas. Por ejemplo las zapatillas voladoras 'PyonPyon' que te permiten saltar más alto y correr más rápido. También ha inventado un sillón para echar siestas que ayuda a energizar el cerebro, se llama 'Cerebrex' y dice que lo usa él mismo todos los días para poder conseguir inventar más cosas aún. Otra de las cosas curiosas que hace Nakamatsu es que saca fotos de todo lo que come desde hace 35 años y anota todos los días cómo se siente para ir viendo que efectos tiene cada comida en su estado de ánimo. Este estudio de la comida que ha consumido durante más de tres décadas le sirvió para ganar el Premio Ig Nobel en 2007. Su invención más conocida en Japón es 'Love Jet', que es una especie de spray estimulante sexual que según Nakamatsu es mucho más potente que la viagra. Nakamatsu dice que esta es una de sus invenciones en las que más esfuerzo ha puesto porque quiere ayudar a que Japón salga de la crisis, quiere ayudar a que los japoneses tengan más hijos y restaurar la pirámide que ahora mismo está totalmente invertida. Lo interesante del 'Love Jet' es que el Dr. Nakamatsu lo vende más barato de lo que le cuesta producirlo, dice que lo hace para ayudar al país, que no hizo el 'Love Jet' para ganar dinero. Lo tiene a la venta en: http://www.nakamats.net/lovejet.html

Por Kirai (http://www.kirainet.com/el-doctor-nakamatsu)



FRIKI GADGET



Pantalla 22" eco-eficiente

MultiSync EA221WMe de NEC Display Solutions utiliza una tecnología de panel altamente eficiente que solo requiere dos tubos de backlight y sin que esto afecte a la calidad de la imagen. Según la empresa, esta pantalla LCD panorámica proporciona un ahorro de energía superior al 30% en comparación con los monitores más convencionales. Al ahorrar dos backlights, el NEC MultiSync EA221WMe muestra una excelente eficiencia energética y dispone de un consumo global de 26 vatios y de tan solo 19 vatios en Modo Eco. Con sus características técnicas, el panel ofrece estupendos ángulos de visión horizontal y vertical de hasta 176 grados (a un ratio de contraste de 5:1) así como un tiempo de respuesta de 5 ms. La nueva tecnología de backlight y su distribución de la uniformidad de la luz altamente efectiva, el brillo de 250 cd/m2 así como el ratio de contraste de 1000:1 garantizan una gran experiencia de visualización. El conector analógico y el interfaz DVI-D digital con HDCP soportan un despliegue flexible para aplicaciones de oficina. **www.nec.com**



Plataformas para procesadores Lynnfield de Supermicro

Flytech trae los nuevos servidores monoprocesador, de gama de entrada de Supermicro. Se trata de soluciones optimizadas para los nuevos procesadores de la serie 3400 Intel Xeon (Lynnfield). Su mejora les posibilita ofrecer más rendimiento, menor consumo energético y todo ello a un menor coste. Esta nueva generación de servidores UP cuenta con hasta 32GB de memoria DDR3, soporta PCI Express 2.0 con SAS 2.0 6Gb/s opcional y gestión remota basada en IPMI2.0 integrados en placa. Así Flytech suma a su oferta diez nuevos SuperServidores basados en seis nuevas placas. Estos modelos conforman un rango que va desde el 5016I-MR de fondo corto (algo más de 35cm), basados en la placa de servidor X8SIL, hasta el 1016I-M6F de alta densidad, con soporte de hasta ocho discos SAS 6Gb/s extraíbles en caliente con IPMI 2.0 de gestión remota integrado en placa. **http://www.flytech.es**



Android al alcance de todos

Con HTC Tattoo, un móvil basado en el sistema operativo Android, ofrece la posibilidad de personalizar el terminal, hardware incluido. El HTC Tattoo es el segundo móvil que incorpora HTC Sense, una experiencia que, centrada en las personas, simplifica y hace más intuitivo el uso del teléfono. Además, se puede diseñar y adquirir carcasas propias proponiendo diseños propios o seleccionándolo entre los diseños más populares el que mejor se adapten. El HTC Tattoo integra los servicios de Google para telefonía móvil: Google Maps, buscador, Google Mail y Android Market, donde se pueden descargar las aplicaciones y juegos más populares. El terminal cuenta con una cámara autofocus de 3,2 megapíxeles, una conexión para cascos de 3,5 mm y una tarjeta de memoria micro SD expandible. **www.htc.com/es**



Clásico por fuera, poderoso por dentro

El nuevo PC 7152 es un potente equipo de sobremesa que cuenta con grandes capacidades técnicas y con espacio suficiente para poder almacenar hasta 1TB de información en su disco duro. Además dispone de 12 GB de memoria RAM (6x2GB). En esta línea, sus componentes técnicos lo convierten en uno de los ordenadores PC más potentes del mercado, puesto que incluye un procesador Intel Core i7 – 920 y placa base PEGATRON IPMTB-GS de triple canal. Dispone de tarjeta de sonido de ocho canales y tarjeta gráfica nVidia GeForce GT230. Para favorecer al máximo la conectividad, el PC 7152 C1, dispone de conexión LAN 10/100/1000 y fireware. El PC 7152 viene con ratón y teclado inalámbricos, aumentando la capacidad de movimientos del usuario, e incluye Windows Vista Home Premium y software de grabador/ reproductor DVD. **www.medion.es**

Centro de entretenimiento digital

El EVA2000 de NetGear es pequeño dispositivo que permite reproducir videos directamente desde Internet, de canales como YouTube, Amazon, CinemaNow, Hulu, Netflix y muchos más, sin necesidad de usar un ordenador. Este nuevo centro digital de entretenimiento digital cuenta con dos puertos USB, un puerto HDMI para alta definición, puerto RCA para televisores analógicos y un puerto Ethernet que se conecta directamente a la red doméstica. Así, se puede acceder a contenidos almacenados en discos duros externos, PCs o streaming desde Internet. El EVA2000 puede conectarse a Internet tanto por cable como por Wi-Fi. En el primer caso, el cable Ethernet se conecta directamente al router; en el caso de la conexión inalámbrica, el dispositivo se instala a través del adaptador inalámbrico EVAW111 de NETGEAR. Una vez conectado, el mando a distancia del EVA2000 permite explorar el contenido desplazándose por el menú o mediante un buscador donde se introducen palabras clave para encontrar contenidos de interés. Además el dispositivo viene con una prueba gratuita del servicio VuNow. **www.netgear.es**





Papyre 5.1 de Grammata, libro electrónico de bolsillo

El Papyre 5.1 es el segundo modelo de e-reader que Grammata lanza al mercado. Posee una pantalla de 5" y se convierte en soporte ideal para reproducir libros o documentos digitales y leerlos con la misma calidad que en papel en cualquier lugar. Sin brillos ni emisión de luz, ofrece una la máxima calidad de lectura gracias a la tecnología E-ink y Viz-plex que no cansa la vista y ofrece una total nitidez. Además, su reducido tamaño (10,5 x 15,5 x 1 cm) y sus 160 gr. de peso, incluyendo la batería, hacen que se puede llevar en cual-quier bolsillo. Ofrece una gran autonomía debido al bajo consumo de energía (hasta 9.000 pasos de página) y la batería de litio que incorpora, lo que evita que el usuario tenga que recargarla en semanas. Por otro lado, Papyre 5.1 presenta una capacidad de almacenamiento de hasta 16 GB, lo que significa que puede albergar hasta 16.000 libros. El producto se comercializa con la biblioteca Grammata Libre compuesta de 500 libros clásicos precargados sin coste adicional **www.grammata.es**

FRIKI GADGET



Adaptadores universales para mini portátiles

Tras el éxito obtenido por la serie de adaptadores universales NB CEC, FSP Group (FSP) presenta ahora dos nuevos productos para mini portátiles: los adaptadores Net 36 y Net 40. Al igual que los anteriores, éstos cumplen con los protocolos CEC (California Energy Comission) y Energy Star Level V, que garantizan que estos adaptadores consumen menos de 0.3W en modo standby y ofrecen una eficiencia del 87%. El Net 36 tiene un voltaje de salida de 12V y es compatible con mini portátiles Asus Eee PC. Por su parte, el Net 40 cuenta con un voltaje de salida de 19V y es compatible con modelos de HP, Dell, Acer, Lenovo, Toshiba, Fujitsu, LG y Samsung. **www.fsplifestyle.com**

WD Scorpio Blue, disco duro móvil de 1TB

Los discos duros WD Scorpio Blue SATA de 2,5" están disponibles en capacidades de 750 GB y de 1 TB, tienen un formato de 12,5 mm y son especialmente adecuados para usarlos en soluciones de almacenamiento portátiles, como los discos duros portátiles USB My Passport Essential SE, presentados recientemente. Ambos discos ofrecen un alto rendimiento, con una tasa de transferencia de 3 gigabits por segundo (Gb/s). Los discos duros WD Scorpio Blue ofrecen un alto rendimiento, un reducido consumo de energía y un funcionamiento sin calentamiento en las aplicaciones portátiles. Están diseñados con prestaciones de WD que los hacen fiables y resistentes a los impactos, a la vez que ofrecen una capacidad y rendimiento líderes del sector. **www.wdc.com**







Vogel's 8000 Series y organiza tus equipos A/V y los cables

No hay nada más frustrante que comprar un nuevo soporte de pared o de pie para la pantalla plana y al colocarlo en casa, darse cuenta de que debido a los antiestéticos cables tanto de la televisión como de los numerosos dispositivos multimedia (reproductores de DVD, consolas, etc.) no crea ese aspecto elegante esperado. Para evitar esta decepción, la gama 8000 Series de Vogel's ofrece varias soluciones. Por un lado la columna para cables, que es ultra delgada (sólo 2 cm) y está disponible en dos longitudes de 64cm y 94cm y puede almacenar hasta 10 cables. Por otro lado el soporte múltiple para A/V, que ofrece un amplio espacio donde poder colocar justo debajo de la pantalla plana todos los equipos A/V, pudiéndose ajustar el soporte a la altura, fondo y ancho que más le convenga según el tamaño de sus dispositivos. Finalmente la cubierta universal para cables (arriba a la derecha) es una alternativa a la columna para cables de tan sólo 2 cm de grosor, fácil de montar y hecha de aluminio. **www.vogels.com**



LCD pequeños y finos

Con un perfil plano de tan sólo 1,7 cm y acabados en negro, Airis pone a la venta nuevos modelos de LCD de 19, 22 y 24 pulgadas con tecnología LED que permite sean las televisiones con menor consumo de energía. Algunos de ellos cuentan con TDT integrado que dará la posibilidad de ver la TDT de alta definición cuando se implante en España. Además, las de 22 y 24 pulgadas son FULL HD (1920 x 1080), lo que permite ver cualquier imagen con la mejor calidad. Además e disponen de acceso CI que hace posible la visión del TDT de pago con ayuda de una CAM (Módulo de Acceso Condicional). Además los modelos de la nueva gama cuentan con euroconector, salida de audio digital coaxial, auriculares, VGA, HDMI, y entrada de PC audio & CI. **www.airis.es**

Altavoces para ordenador de 200 vatios

El Expressionist Ultra (MX6021) de Altec Lansing, división de Plantronics, combina un sofisticado diseño con una reproducción de audio precisa y potente para música, juegos y películas. Con 200 vatios continuos (RMS), el Expressionist Ultra cuenta con cinco amplificadores digitales y cinco drivers independientes para una explosión de música verdaderamente afinada. Cada driver del altavoz - los altavoces de medio alcance de 3", los bafles para agudos de neodimio de 1" y el subwoofer de largo alcance de 6 1/2" - funciona de manera independiente. El resultado es un audio muy detallado y unos revolucionarios graves con el sonido más auténtico. **www.alteclansing.com**



AgfaPhoto AS 1110, AS 1111, AS 1300, AS 1300 Pro

Sagem Communications lanza una nueva gama de escáneres Agfaphoto, formada por cuatro modelos ligeros y extremadamente compactos. Los modelos AgfaPhoto AS 1110 y AS 1111 (46x156x38 mm) pueden escanear fotos de 10 x 15 en 5 segundos, con una resolución de 1800 x 1200 píxeles y transferirlas a un marco digital o a un ordenador personal. Los modelos AS 1300 y AS 1300 Pro (47x274x33,8 mm) tienen un enfoque más profesional para usarlos con un PC. Además del escaneo de imágenes en formato JPG, BMP, TIF o PCX, permiten escanear tarjetas de visita y documentos empresariales A4 a una velocidad de tres páginas por minuto, con una resolución de 600 x 600 dpi y transferirlos a través de formatos PDF, RTF, Word o HTML. Y el modelo AS 1300 Pro ofrece además la función de búsqueda en PDF que indica que el documento escaneado (resultado en formato PDF) ha sido procesado a través de reconocimiento óptico de caracteres (OCR) y permite buscar el archivo por apariciones de una palabra o una frase, haciendo mucho más fácil la búsqueda de un documento.
www.sagem-communications.com / www.agfaphoto.com

FRIKI GADGET

Sentinel Advance Gaming Mouse

Diseñado para 'buscar y destruir': así es como se presenta el primer ratón de la serie profesional de ratones gaming de CM Storm, el Sentinel Advanced. Con agarre y control milimétrico, hará las delicias de los expertos en gaming. Distribuido por Sistemas Ibertrónica, se trata de un producto creado por gamers para gamers. Como todos los productos CM Storm incorpora las ya conocidas Storm Tactics, que proporcionan fuerza, seguridad y control al usuario. Entre sus múltiples características destaca que sus 5600 DPI Storm Tactical Sensor utilizan un doble sensor láser, procesos Doppler Effect y seguimiento a tiempo real. Dispone de un botón duro que aporta una fuerza añadida al Sentinel, haciendo que los disparos sean más precisos y certeros. Añade una amplia variedad de configuraciones y funcionalidades, permitiendo almacenar hasta cinco perfiles distintos en la memoria interna del ratón, además de poderlos intercambiar durante su uso de forma inmediata, desde el propio ratón, sin interrumpir el juego. La tecnología Octoshade de los LEDS ofrece la posibilidad de modificar los colores para identificar en que perfil está actuando o simplemente obtener una mayor luminosidad. Por su parte la pantalla OLED permite personalizar los logotipos de los clanes que se cargan y muestran en el propio ratón. Incluye el sistema de seguridad StormGuard para salvaguardarlo de robos en eventos como las LANparties o ambientes concurridos. **www.ibertronica.es**





JournE touch, nuevo Tablet multimedia de Toshiba

El JournE touch de Toshiba es un Tablet PC con conexión inalámbrica y pantalla táctil. Su sencillo uso permite navegar por Internet y descargar contenidos digitales usando únicamente la yema de un dedo. El dispositivo garantiza el acceso a Youtube de una manera rápida y sencilla a través de la red inalámbrica WLAN asegurando información y entretenimiento.Con una pantalla LCD de 7" 16:9 y retroiluminación LED, el JournE touch dispone de teclado digital y viene con un puerto USB y una conexión HDMI que permite conectar el equipo con un televisor o un portátil y poder así visualizar el contenido en una pantalla más grande. Sus medidas son de 189 x 133,6 x 14 mm y cuenta con una batería de polímero de litio que puede durar hasta 14 horas, tiempo suficiente para reproducir música. Para la reproducción de vídeos o la navegación por la red el tiempo se limita a dos horas. Posee una memoria interna de 1 GB que puede ampliarse con una tarjeta SD hasta 32 GB. **www.toshiba.es**

Tuitea tus garabatos

¿Eres una de las 12 millones de personas registradas en Twitter? ¿Intentas decir algo interesante, provocador o gracioso en tu estatus? ¿Estás limitado por 140 caracteres? Bamboo Mini 'Drawtweet' es una aplicación que permite a los usuarios decir más en un solo tweet. Con ella, se puede hacer un garabato o un croquis y compartirlo a través de Twitter, red social de micro-blogging. Drawtweet proporciona características simples y útiles para dominar el lápiz digital Bamboo. Con un click en el botón 'enviar', el dibujo se envía a Twitter y se tuitea de forma instantánea a los followers. El tweet contendrá un link a un servicio llamado Twitpic, donde se podrá ver el dibujo. Buscando '#Drawtweet' se pueden ver en tiempo real qué otros dibujos han hecho otras personas utilizando Drawtweet y su tableta Wacom Bamboo. Drawtweet también incluye una galería de imágenes donde poder ver los dibujos recientes de otros usuarios. **www.wacom.eu/bamboo**



Conmutadores Gigabit para la red doméstica

El continuo desarrollo de las nuevas tecnologías ha llevado a incluir puertos de red en muchos productos electrónicos, como los televisores. Esto ha dado lugar a un notable incremento de dispositivos y aplicaciones con capacidad de conexión en red en el hogar. En respuesta a esta tendencia, Belkin presenta una nueva gama de conmutadores Gigabit de alto rendimiento y bajo consumo con cinco y ocho puertos. Los nuevos conmutadores permiten conectar varios dispositivos, como una X-BoX, una PlayStation y un reproductor de Blu-Ray a su red sin añadir más cableado. Además se trata de dispositivos de bajo consumo que sólo suministran alimentación a los puertos cuando detectan que se ha conectado otro dispositivo. Así los puertos calculan la energía con la que deben funcionar en función de la longitud del cable conectado y entran en modo de espera tan pronto como se apaga el dispositivo conectado. Estos nuevos conmutadores también son muy silenciosos, ya que funcionan sin un ventilador, lo que reduce aún más el consumo energético. Todos los puertos cuentan con detección automática y son dúplex, de modo que a pleno rendimiento ofrecen hasta 2000 mbps (1000 mbps de entrada y salida simultáneos) por puerto. El estándar IEEE802.3x garantiza continuidad y una gestión eficiente del flujo de datos. **www.belkin.com**









Teléfono para mayores

Botones grandes y bien visibles, teclas de marcación directa con números de emergencia y un menú sencillo de utilizar. Estas son las características de AMICO de Brondi, un teléfono móvil pensado especialmente para facilitar la comunicación de las personas mayores o de aquellas que cuentan con carencias visuales. Distribuido por Elta Hispania, el Brondi Amico dispone de un botón especial de emergencia SOS situado en la parte posterior que al pulsarlo realiza una llamada al número que el usuario haya memorizado previamente como, por ejemplo, el servicio de emergencias. A ello se suman otras prestaciones especialmente indicadas para personas con una visibilidad reducida, como pantalla y teclado con retroiluminación o la función de linterna para iluminar cualquier entorno. **www.eltahispania.com**

Terminator: The Sarah Connor Chronicles podría tener una película

Cancelada tras dos temporadas de emisión en Fox, la serie 'Terminator: The Sarah Connor Chronicles' parece ser que podría volver en formato película, según nos llega vía Aceshowbiz (**www.aceshowbiz.com**). Y no se trata de un rumor infundado sino que ha sido uno de sus protagonistas, el actor Thomas Dekker que interpretaba a John Connor el que reveló en una entrevista a TV Addict la posibilidad de que Terminator tuviera continuación en película para DVD. Así que los seguidores, que se han movilizado a través de varias campañas para convencer a Fox de rectificar su decisión, podrían estar de enhorabuena. En ella se podrían dar respuesta a las cuestiones que han quedado abiertas ante la inexistencia de una tercera temporada como si Sarah Connor en el futuro habría sobrevivido o estaría muerta. A la espera de una decisión en firme, los de SciFi Scoop animan a los seguidores a participar en alguna de las múltiples campañas que hay en marcha pues cabe la posibilidad de que tanta movilización realmente sirva de algo y defina el futuro de la serie. Se puede consultar más información en **www.savethescc.com** e incluso seguirlos en Twitter: **http://twitter.com/savethescc** <





Matt LeBlanc hará de sí mismo

La cadena Showtime ha fichado a Matt LeBlanc (conocido por todos por su interpretación del entrañable Joey Tribbiani de 'Friends') para protagonizar 'Episodes', una comedia satírica. Según informa la misma cadena en su página web, el actor estadounidense se interpretará a sí mismo en la serie, que trata de una pareja que protagoniza una exitosa comedia en Inglaterra y que decide cruzar el charco para triunfar. Pero cuando el equipo de la comedia llega a Hollywood se percata de que las cosas no son lo que esperaban. Pronto se ven engañados por los ejecutivos americanos que les propone una nueva adaptación de la serie que conlleva cambios como la substitución del protagonista erudito británico por Matt LeBlanc. Poco a poco se van hundiendo en las arenas movedizas del negocio televisivo. David Crane, co-creador de 'Friends' es uno de los artífices del proyecto en el que también estará Jeffrey Klarik ('The Class', 'Mad About You'). 'Episodes', una coproducción de Showtime y la BBC, contará inicialmente con seis episodios que se rodarán este invierno entre Londres y Hollywood para su estreno en 2010 en ambas cadenas.

"Jeffrey y David tienen una gran idea. Me encanta", explicó el propio LeBlanc, según las declaraciones que se recogen Hollywoodreporter.com. "Me siento realmente emocionado de trabajar con Showtime y la BBC. Y estoy muy contento de tener el papel pues ver a otro interpretando a Matt LeBlanc podría haber sido devastador". Tras el gran éxito obtenido con 'Friends', serie que se emitió desde 1994 a 2004, el actor protagonizó el spin-off de la misma, 'Joey', una serie que narraba la vida del personaje Joey Tribbiani en Los Ángeles junto a su sobrino y una de sus hermanas. <



A por la tercera parte



Habrá una tercera entrega de Kill Bill, según ha confirmado Quentin Tarantino. La noticia nos llega vía **http://cineconmcfly.com.ar** y ha sido él mismo quien lo ha desvelado en una entrevista televisiva en el show italiano 'Parla con me' de Rai Uno donde se encontraba promocionando su película 'Malditos bastardos', de ha confirmado que habrá una película que narrará el antes o el después de la presente, extremo aún sin concretar. Y de la que al parecer no habrá ningún tipo de continuación es de 'Pulp Fiction', la que es considerada por muchos como su obra magistral.

De momento lo que sí que parece seguro es que "la novia volverá a luchar", afirmó Tarantino seguido por los aplausos del público. Sin fecha aún para la tercera parte, una de las grandes incógnitas es cómo se las apañará sin el actor David Carradine, siendo como era el personaje Bill. Uma Thurman volverá a ser la protagonista de 'Kill Bill vol.3', filme que al parecer narrará la venganza de alguno de Los 88 maníacos, los sicarios a los que La Mamba Negra/la novia asesinó o dejo malparados.

Y otra confirmación de una tercera entrega hace referencia a 'Transformers'. La continuación de la película llegará en el 1 de julio de 2011, ha anunciado Michael Bay, según nos llega a través de Aeromental.com (**http://www.aeromental.com/2009/09/16/michael-bay-dirigira-transformers-3-pain-gain-y-bad-boys-3**). Y es de la información publicada en el sitio web oficial del director -**www.michaelbay.com**- se deduce que a esta decisión se habría llegado tras reunirse él mismo con Steven Spielberg y Ehren Kruger para discutir ideas para 'Transformers 3'. En su web, Bay dedica unas líneas a Megan Fox, a quien le pide que vuelva, que le promete que ningún robot alienígena la herirá durante el rodaje.

Además, dos películas dirigidas por Bay, 'Pain & Gain' y 'Bad Boys 3' podrían llegar a la gran pantalla antes que la tercera parte de la película de robots. Hasta ahora las declaraciones de Bay en torno al rodaje de 'Pain & Gain' parecían descartar que pudiera rodar 'Transformers 3' en breve. Pero al parecer todo le cuadra en la agenda. 'Pain & Gain' trata de un grupo de culturistas con una adicción a los esteroides, a las strippers y el dinero rápido que además se convirtieron en expertos en el uso de una particular herramienta de motivación: la tortura.

En fin, que ambos directores tienen grandes planes para los próximos años. <



Ya ha regresado House

'House' ha regresado a Fox y lo ha hecho a principios de octubre, en su horario habitual, pero en versión original subtitulada y 12 días después del estreno en Estados Unidos de la sexta temporada de la serie que, el pasado 21 de septiembre, logró alcanzar una audiencia record de 17 millones de espectadores. Esta nueva y esperada entrega comienza con un episodio extraordinario, de hora y media de duración, ambientado en el psiquiátrico en el que el protagonista ingresa al final de la quinta temporada. Concebido como si fuera una película, el episodio rindió homenaje al cine al inspirarse en 'Alguien voló sobre el nido del cuco', filme de Milos Forman por el que Jack Nicholson ganó un Oscar en 1975.

Se trató de un estreno excepcional que, a finales de octubre y en prime time de forma regular, se volvió a repetir el episodio especial de hora y media ya en versión doblada. También se comenta que la actriz Jennifer Morrison, que interpreta a la doctora Allison Cameron en 'House', podría irse de la serie a mediados de la sexta entrega. Después de cinco años, los responsables de la serie habrían decidido prescindir de la inmunóloga del hospital Princeton-Plainsboro por razones creativas, según han publicado varios medios norteamericanos como Entertainment Weekly. <



Las mil y una posibilidades del DNIe



Todos aquellos que han acudido a una comisaría a solicitar el DNI en el último año ya disponen de un carnet electrónico con un montón de utilidades que pocos utilizamos: pedir documentación, realizar trámites y consultas... Y todo sin salir de casa.

Internet ha abierto un mundo de infinitas posibilidades para realizar multitud de tareas desde casa, únicamente con un ordenador con conexión a Internet: compras, descargas, conferencias, llamadas, gestiones... Para realizar algunas de ellas con total seguridad resulta esencial garantizar la identidad de la persona. En este sentido, se han tomado un conjunto de medidas legislativas que han permitido la creación de instrumentos capaces de acreditar la identidad de las personas que intervienen en una comunicación electrónica y, a su vez, asegurar la procedencia y la integridad de los mensajes. El más conocido es el DNI electrónico (DNIe), durante mucho tiempo conocido popularmente como el DNI "nuevo", que ya está totalmente asentado en España. Desde noviembre de 2008, todos los documentos identificativos expedidos en nuestro país se corresponden con la nueva normativa y ya son más de 12 millones, según datos de la Policía Nacional. Teniendo en cuenta que tienen que renovarse cada 10 años, estará totalmente implantado antes de 2020. Eso sí, los mayores de 70 años pueden mantener sus documentos an-



tiguos, ya que no tienen obligación de cambiarlo. Su primera función sigue siendo la identificación del ciudadano, pero este nuevo carnet integra un circuito electrónico en forma de chip. Gracias a él, es capaz de ofrecer una serie de servicios hasta ahora impensables, como acreditar la identidad de la persona a distancia y hacer las funciones de una firma digital. La renovación estética también es patente: ha cambiado su soporte tradicional, una cartulina plastificada, por una tarjeta de material plástico, que permite integrar el circuito.

Toda la información

El famoso chip, similar al de las tarjetas de crédito, contiene multitud de información sobre la identidad de la persona. Por ejemplo, integra un certificado electrónico para autenticar la personalidad del ciudadano, otro que permite firmar electrónicamente con validez jurídica y un tercero de la Autoridad de Certificación emisora. Además, también guarda la clave para su utilización, la huella dactilar, la fotografía y la firma manuscrita, todas ellas en formato digital.

Por último, incluye todos los datos de filiación del ciudadano. Toda esta información se utiliza para garantizar que la persona que lo emplea es quien dice ser. Por ello, también se han tomado una serie de medidas que intentan evitar la falsificación de los carnets. En primer lugar, se han utilizado tintas especiales, relieves y fondos de seguridad que hacen que sea más difícil de imitar. En segundo, los datos del chip están encriptados y se incluye la certificación de la Dirección General de la Policía.

Aunque todavía su utilización es bastante limitada (en gran medida, por el desconocimiento de los servicios que ofrece), el DNIe tiene multitud de funciones. Entre ellas, destacan por ejemplo las compras firmadas a través de Internet, para que no haya duda del comprador; la realización de trámites con las Administraciones Públicas, independientemente de la fecha y hora y ahorrándose las incómodas colas; transacciones más seguras en entidades

>>> INICIATIVA CERES

En España, las Administraciones han apostado por Internet para comunicarse con los ciudadanos desde antes de la llegada del DNIe y, por ello, han creado páginas web con toda la información de interés público que pueden ofrecer de cara a facilitar el intercambio de información. Antes de que el carnet electrónico se convirtiera en la herramienta más útil para realizar trámites a distancia con la administración, la Fábrica Nacional de Moneda y Timbre puso en marcha la iniciativa Ceres, que establece una Entidad Pública de Certificación para garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y Administraciones Públicas a través de las redes abiertas de comunicación como Internet. De su proceso de creación de una firma electrónica ya hemos hablado antes, pero cabe destacar que, pese a la implantación del DNIe, todavía se sigue solicitando este certificado. Actualmente, más de dos millones de personas lo mantienen activo, según el Ministerio de Economía y Hacienda, y el número crece día a día. La funcionalidad de los dos es la misma, pero este certificado está únicamente disponible en el ordenador en el que ha sido instalado.



>>> CON CITA PREVIA

Para hacerse por primera vez el DNI o renovarlo hay que pedir una cita con la comisaría correspondiente, que se puede concertar a través de Internet en la dirección www.citapreviadnie.es o por teléfono en el 902 247 364. Lo positivo de este sistema es que a cada ciudadano se le asigna una fecha y hora a la que acudir con la documentación necesaria y así no tiene que esperar ninguna cola. Es importante tener en cuenta que en algunos lugares también se reservan algunos números para gente sin cita. La realización del DNIe es, a su vez, mucho más rápida de lo que era tradicionalmente y se invierte de media la mitad de tiempo, 10 minutos, en esta tarea. Por si eso fuera poco, no hay que esperar un mes, como antes, para recoger el nuevo documento, que se entrega el mismo día.

EL CHIP, SIMILAR AL DE LAS TARJETAS DE CRÉDITO, CONTIENE MULTITUD DE INFORMACIÓN SOBRE LA IDENTIDAD DE LA PERSONA. INTEGRA UN CERTIFICADO ELECTRÓNICO PARA AUTENTICAR LA PERSONALIDAD DEL CIUDADANO, OTRO QUE PERMITE FIRMAR ELECTRÓNICAMENTE CON VALIDEZ JURÍDICA Y UN TERCERO DE LA AUTORIDAD DE CERTIFICACIÓN EMISORA. TAMBIÉN GUARDA LA CLAVE PARA SU UTILIZACIÓN, LA HUELLA DACTILAR, LA FOTOGRAFÍA Y LA FIRMA MANUSCRITA.



bancarias; y su utilización como tarjeta de entrada a algún edificio, de acceso a un ordenador personal o para participar en una conversación vía Internet con la certeza de que el interlocutor es realmente la persona con la que queremos hablar.

Es muy interesante recalcar que, además, utilizar el DNIe para alguna de estas funciones, sobre todo las de trámites y solicitudes con la Administración, facilita la tarea. Y es que, si antes había que personarse en la oficina correspondiente, esperar el turno y presentar determinados documentos y certificados para llevar a cabo algunas acciones, ahora en algunos casos no es necesario. La solicitud se hace desde casa y el papeleo se reduce significativamente, ya que si esa información existe en cualquier Unidad de la Administración, la entidad en la que se esté tramitando un caso concreto también podrá acceder a ella con la autorización del ciudadano. Por el momento, es imposible acceder a todas estas aplicaciones y las disponibles están muy dispersas entre las distintas páginas web de las Administraciones Públicas. Pero todavía quedan unas semanas para que todos los servicios se adapten a la vía telemática dentro del plazo establecido por ley. Por eso, muchos organismos siguen adaptando su oficina virtual al certificado y la firma electrónica. Algunos de los que más se han volcado en trasladar sus trámites a Internet han sido la Seguridad Social, Hacienda y el INEM, y ahora es mucho más rápido y sencillo solicitar un extracto de la vida laboral o incluso consultar los puntos del carné de conducir a través de la página de la DGT. Pero los servicios no se limitan únicamente a las Adminis-

>>> LECTORES COMPATIBLES CON EL DNIE

A la hora de comprar un lector hay que asegurarse de que cumpla el estándar ISO 7816 (1, 2 y 3).

- **Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1).**
- **Soporta velocidades de comunicación mínimas de 9.600 bps.**
- **Soporta los estándares:**
  - **API PC/SC (Personal Computer/Smart Card)**
  - **CSP (Cryptographic Service Provider, Microsoft)**
  - **API PKCS#11**



>>> COMPLEMENTOS PARA EL DNIE

El DNI electrónico no funciona solo: tiene que recurrir a hardware y software para sacarle todo el partido a sus servicios. Por ejemplo, es necesario tener a mano un ordenador con conexión a Internet y sistema operativo Windows, Mac, Linux y Unix. Además, es imprescindible utilizar el navegador Internet Explorer, Mozilla Firefox o Netscape. El último elemento de software indispensable para poder interactuar adecuadamente con el carnet son unos módulos criptográficos que ha de tener instalado el ordenador: en un ordenador con Windows, debe estar instalado un servicio que se denomina "Cryptographic Service Provider" (CSP). En los entornos UNIX / Linux o MAC su nombre es "PKCS#11". Puedes descargar cualquiera de ellos directamente desde la página web del DNI electrónico www.dnielectrónico.es/descargas. Con todo esto instalado, sólo hay que hacerse con un lector de tarjetas inteligentes (por USB, integrado en el teclado o a través de una ranura PCMCIA).



Imagen cambiante grabada en láser.

traciones Públicas, y ya hay entidades financieras que ofrecen la posibilidad de utilizar su documento de identidad como sustituto de una tarjeta de crédito o débito. Entre ellos, muchas cajas de ahorros y bancos.

Mucho más sencillo

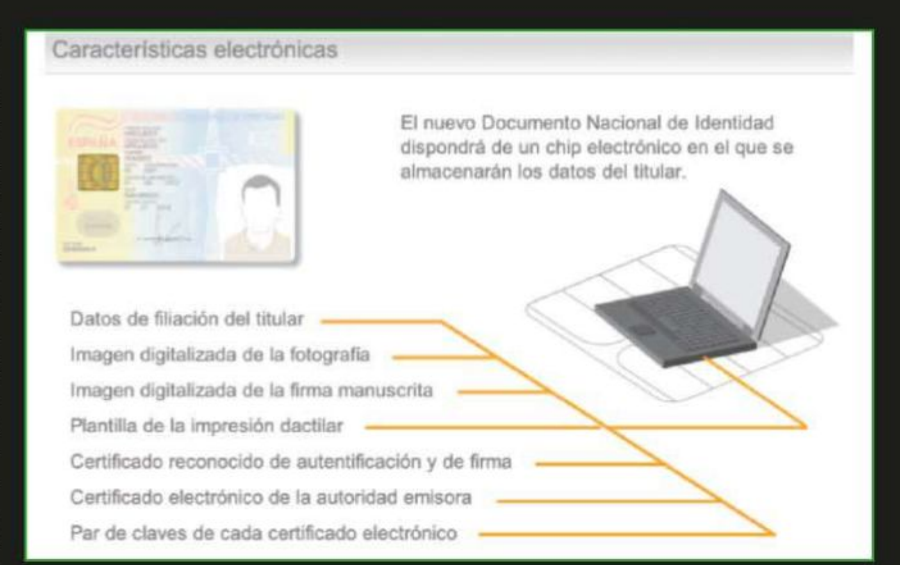
A nivel usuario, para utilizar el DNIe desde el ordenador hay que utilizar un PIN, que se entrega en un sobre ciego a cada ciudadano en el momento de hacerse el carnet. Este número puede cambiarse desde cualquiera de los Puntos de Actualización del DNIe (PAD) que existen en las oficinas de expedición. En ellos, si se conoce el código anterior sólo hay que escribirlo y elegir uno nuevo. En caso contrario, o cuando se ha bloqueado el carnet porque se ha introducido una clave errónea varias veces, la identificación se lleva a cabo a través de la huella dactilar. Una última opción, más sencilla y cómoda porque no exige desplazamientos, es hacerlo desde un ordenador con lector de tarjetas mediante un proceso telemático.

Hasta la llegada del DNIe, conseguir un certificado digital que constatara

la identidad del usuario en su intento por realizar diversos trámites administrativos por Internet era una odisea. El principal inconveniente de ese primer paso hacia la "oficina digital" era que, para conseguirlo, había que tomarse muchas molestias: primero solicitarlo a través de Internet, luego personarse en una oficina de registro, posteriormente descargar e instalar el certificado en el ordenador... y, además, con la incomodidad que suponía que siempre haya que realizar los trámites desde el mismo equipo. En definitiva, qué duda cabe que es mucho más sencillo renovar el DNI y que lo único que haga falta sea utilizarlo. Eso sí, es necesario un dispositivo electrónico preparado para leer el chip del carnet. Actualmente, se venden en varios formatos, por ejemplo, en forma de un adaptador que se coloca en uno de los puertos USB del equipo o integrado en un teclado. Además, su precio ronda los 20 euros, así que es bastante asequible.

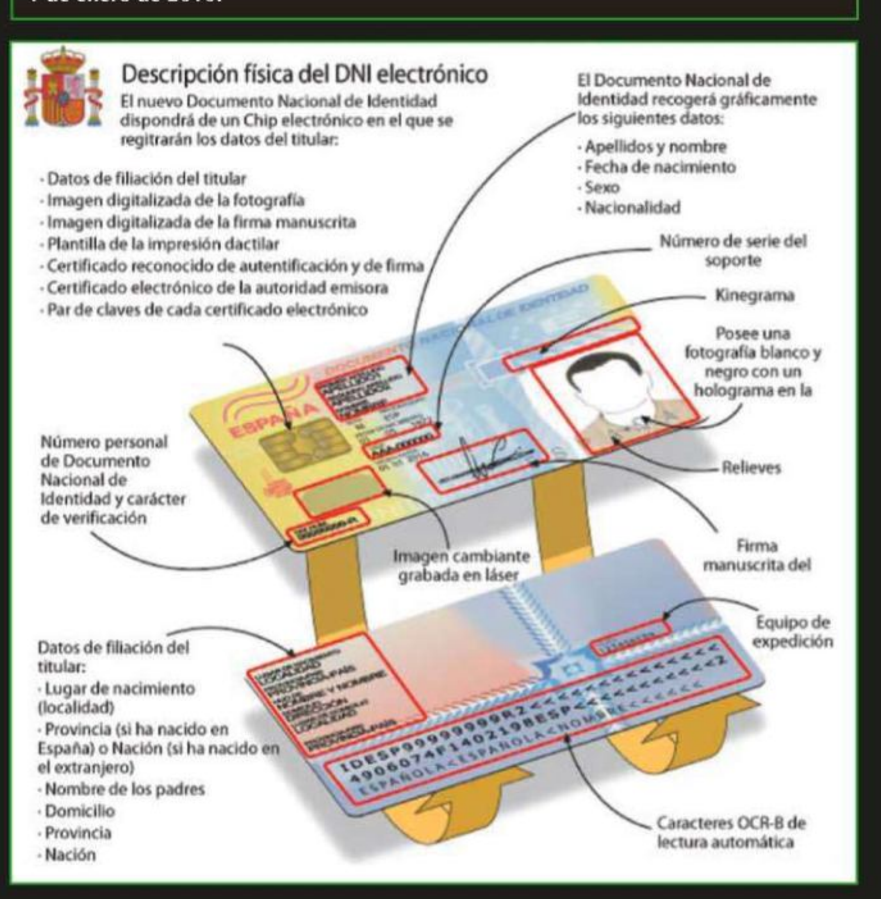
MUCHOS ORGANISMOS SIGUEN ADAPTANDO SU OFICINA VIRTUAL AL CERTIFICADO Y LA FIRMA ELECTRÓNICA. ALGUNOS DE LOS QUE MÁS SE HAN VOLCADO EN TRASLADAR SUS TRÁMITES A INTERNET HAN SIDO LA SEGURIDAD SOCIAL, HACIENDA Y EL INEM, Y AHORA ES MUCHO MÁS RÁPIDO Y SENCILLO SOLICITAR UN EXTRACTO DE LA VIDA LABORAL O INCLUSO CONSULTAR LOS PUNTOS DEL CARNÉ DE CONDUCIR A TRAVÉS DE LA PÁGINA DE LA DGT.

Todos aquellos ciudadanos que ya tienen su carnet y quieren sacarle todo el partido pueden consultar la página web oficial del DNIe, www.dnielectronico.es. Dentro de ella se detallan todas las aplicaciones, todas las administraciones y todos los servicios a los que puede acceder el ciudadano sin moverse de casa. Y también hay una amplia y completa explicación de cómo se usa. Si tiene alguna duda, seguramente encontrará todas las respuestas en la sección de preguntas frecuentes y, si no, siempre puede hacer una llamada al teléfono de atención al cliente.



>>> LEGISLACIÓN

La ley se ha puesto de parte del DNIe y ha favorecido e impulsado su uso. Tanto es así que, el Plan Avanza, una de las grandes apuestas del Gobierno para desarrollar la Sociedad de la Información, cuenta entre sus puntos de interés con esta identificación. Aun así, hay una ley específica que respalda esta tecnología, la 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Con ella, se garantiza que todos los ciudadanos puedan acceder a los servicios de las distintas administraciones (central, autonómica y local) a través de la Red. El plazo previsto para que el acceso sea total está a punto de concluir, ya que se estableció que todo debería estar listo el 1 de enero de 2010.



OFERTA DE SUSCRIPCIÓN

25% DE DESCUENTO

12 números a un precio único 44,55 euros

TRUCOS WINDOWS: RECUPERAR DATOS BORRADOS POR ERROR

@RROBA 146

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

INTERNET CÓMO FUNCIONA GOOGLE

LATEX EDICIÓN DE TEXTOS PROFESIONAL AL ALCANCE DE CUALQUIERA

PROGRAMACIÓN JOOMLA A TU MEDIDA

TECNOLOGÍA NAC REDES SEGURAS Y MÁS CONTROLADAS

COMPARATIVA

Los antivirus a examen

Y ADEMÁS... Cortafuegos de aplicaciones web | CURSO DE JAVA ÚTIL | RETROINFORMÁTICA Discos y memorias encriptadas

Más fácil en www.mcediciones.com

Envía este cupón a:



MC Ediciones, S.A.
Passeig de Sant Gervasi, 16-20
08022 Barcelona

Precio ejemplar 4,95 euros
Suscripción España 44,55 euros
Suscripción Europa 103,95 euros
Suscripción resto mundo 163,35 euros.

☐ Deseo suscribirme a @rroba por un año (12 números) al precio especial de 44,55 euros

Nombre y apellidos .... NIF o CIF ....

Dirección .... Teléfono ....

Población .... Provincia .... C.P. ....

Email ....

Para mayor comodidad puede suscribirse a través de nuestra web: www.mcediciones.com / suscripciones@mcediciones.com

FORMA DE PAGO

☐ Adjunto talón bancario

☐ Tarjeta de crédito

☐ VISA (16 dígitos) ☐ American Express (15 dígitos)

Tarjeta nº

Caducidad

Titular tarjeta o cta. cte.

Firma

☐ Domiciliación bancaria (Datos Banco/Caja)
Con renovación automática hasta su orden.

Banco o caja

Entidad oficina d.c. nº de cuenta

Tras el acrónimo de NAC se descubre una tecnología de control de acceso con grandes posibilidades que consigue evitar, principalmente, episodios desagradables vinculados con la seguridad de la redes.

Redes seguras y más controladas





Preservar la confidencialidad y la integridad de la información es una necesidad vital para cualquier entorno, ya sea corporativo o residencial. En este contexto, el propósito de cualquier infraestructura TIC es erigir sistemas que protejan contra los accesos no permitidos, sin que ello entorpezca la entrada a los usuarios que sí están autorizados. Basta con pensar que la simple denegación de dicho acceso frente a un ataque ya no es aceptable, y que las redes de ahora, además de rechazarlo, tienen que asegurar la continuidad del negocio.

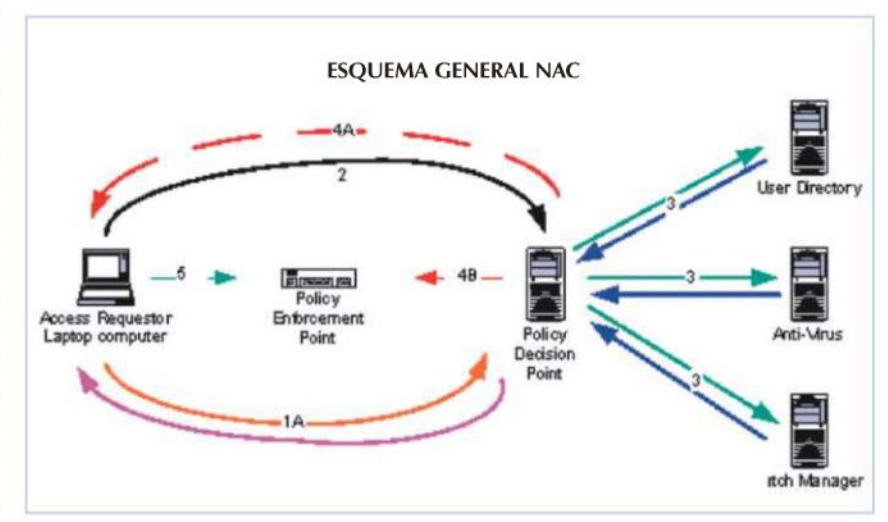
El planteamiento descrito líneas más arriba permite deducir que la seguridad en las redes continúa siendo una máxima fundamental por parte de los responsables de informática y comunicaciones de cualquier organización, dado que tienen que enfrentarse a un amplio y diversificado número de riesgos que pueden provenir tanto de elementos internos como externos. Y es que, en estos instantes, donde todo está interconectado, cualquier riesgo se traslada a millones de equipos y de dispositivos en cuestión se segundos, y los sistemas de seguridad tienen que reaccionar al instante. Ante este panorama, es preciso apostar por soluciones que resulten lo más completas posibles, con dispositivos de detección y prevención de intrusos, securización de puestos de trabajo y servidores, control de admisión, seguridad en transmisión de voz, contención de ataques de tipo denegación de servicio, protección en entornos Wi-Fi, gestión de identidades en red o sistemas de monitorización y análisis, entre otros.

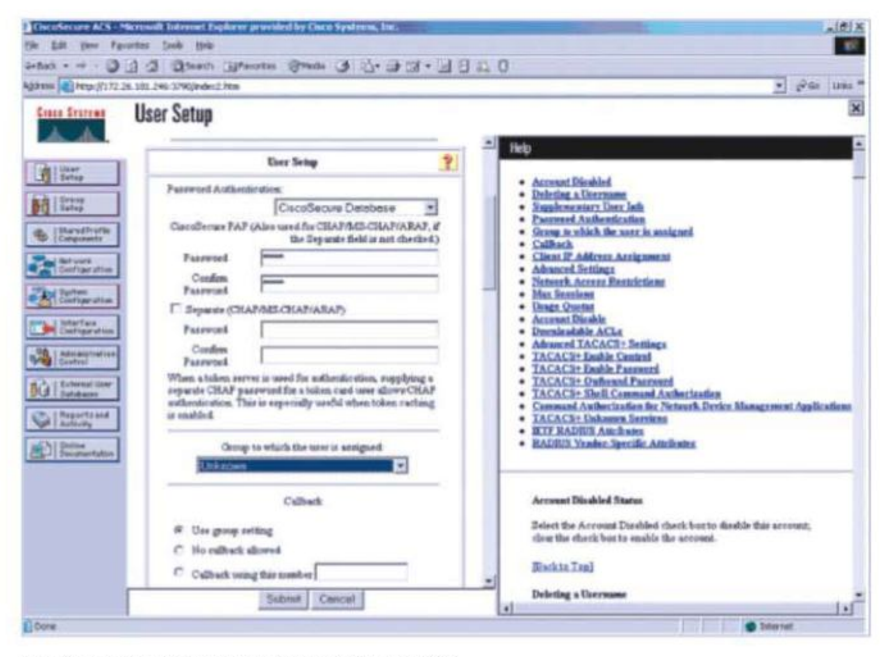
La defensa más eficaz para afrontar estos ataques, dada su complejidad y rapidez de propagación, pasa por minimizar precisamente estos riesgos en la propia red. La tecnología NAC (Network Admission Control), a este respecto, es fundamental para cerrar el paso a los usuarios no deseados, al integrar el cumplimiento de las políticas de admisión, el software antivirus y los recursos de red que mejoren radicalmente la seguridad. Además, neutraliza todo tipo de amenazas y proporciona disponibilidad y continuidad en el negocio, al tiempo que simplifica la gestión de las redes actuales. Así, y gracias a NAC, los routers, los concentradores VPN, los conmutadores y las soluciones Wi-Fi pueden participar conjuntamente en el proceso de admisión o denegación del dispositivo desde el que el usuario desea acceder. Para lograrlo, los recursos de red se comunican con los servidores de autenticación que, de manera opcional, pueden conectarse a los servidores de gestión de políticas de seguridad, de antivirus o de auditoría para comprobar la identidad y el nivel de protección de cada uno de los equipos.

Aunque en un primer instante fue una tecnología destinada a las grandes cuentas, de forma paulatina se ha extendido a las pequeñas y medianas empresas también. La clave está en que NAC es una solución sencilla de utilizar y que proporciona acceso a un amplio abanico de recursos y datos desde cualquier dispositivo y localización.

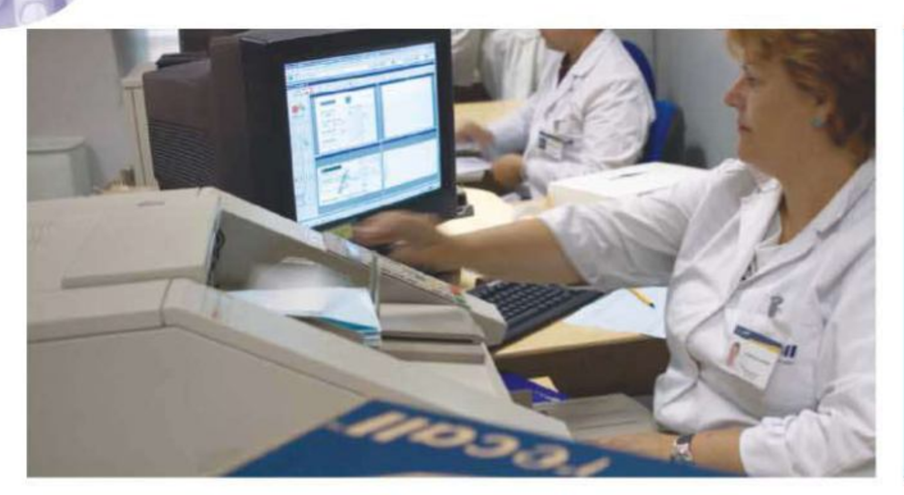
Una tecnología prometedora

Cuando se habla de tecnología NAC, es preciso reparar en la arquitectura (Control de Acceso a la Red) que regula la entrada de los usuarios a la red en el punto de acceso, verificando, por un lado, su identidad, y por otro, el cumplimiento de las políticas de seguridad que cada organización ha definido. Dicha arquitectura, asimismo, establece lo que cada usuario puede hacer, la información que tiene derecho a manejar y los sistemas o recursos que puede utilizar. Es decir, se trata del conjunto de equipos y software que implementan políticas de control de acceso a las LAN y VPN, las oficinas remotas y los puntos inalámbricos, basándose para ello en la identidad del usuario que quiere entrar en la red. Por otro lado, una solución NAC asienta sus cimientos en cuatro principios esenciales que son: la autenticación y la evaluación,





Configuración del usuario de Cisco Secure ACS



>>> VENTAJAS DE LA TECNOLOGÍA NAS

- **Continuidad del negocio.**
- **Red de trabajadores móviles más amplia.**
- **Operaciones de integración con una inversión mínima.**
- **Gestión cómoda y completa a partir de una sola consola centralizada.**
- **Administración autorizada de "parches".**
- **Control de los usuarios que acceden a la red y sus recursos**

la imposición de políticas de seguridad, la cuarentena de puestos y la gestión centralizada. En cualquier punto de entrada, la aplicación se encarga de identificar a los usuarios y los dispositivos en red, evaluando su papel, comprobando el cumplimiento de las políticas establecidas y concediendo los privilegios correspondientes. Así, aquellos que no cumplan con los requisitos establecidos quedan bloqueados y, por tanto, en cuarentena. Además, las actualizaciones de antivirus y anti-spyware se administran automáticamente y se instalan en toda la organización.

Aunque fabricantes de seguridad, de redes y de conectividad han manifestado abiertamente su interés por las arquitecturas NAC, lo cierto es que todavía no son muchos los que se han decidido a implantarla de forma completa. Se trata de una situación que, por otro lado, explicaría el éxito de las soluciones basadas en appliances, mucho más sencillas y capaces de reducir esfuerzos y costes de manera significativa. El otro inconveniente que NAC presenta es que afecta a los sistemas a todos los niveles, desde los elementos de red hasta los los switches, los routers y los cortafuegos, pasando por los equipos de los usuarios y su software, lo que puede originar incompatibilidades.

A pesar de ello, NAC ha suscitado un gran interés y se prevé un crecimiento espectacular en los próximos años. A este respecto, la consultora Infonetics Research señaló en un informe que las ventas de estos productos pasarían de los 323 millones de dólares de 2005 a los 3.900 millones en 2008, lo que representa un aumento del 1.100% en tres años.

La seguridad

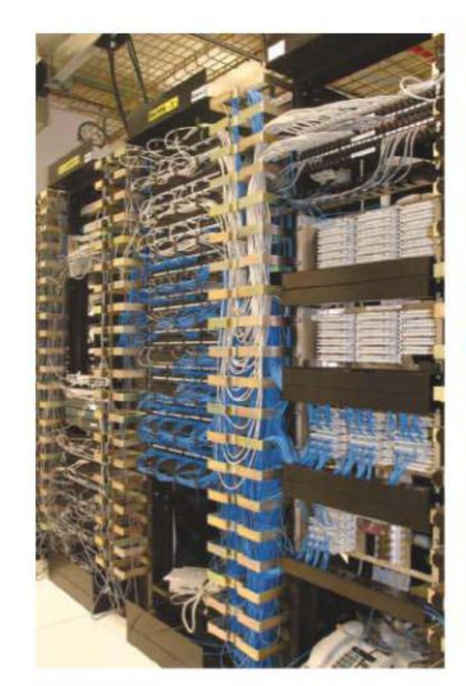
Uno de los aspectos más importantes para asegurar la protección de las redes es el que se refiere a la necesidad de concienciar a los usuarios de las reglas que cada organización o entorno tiene establecidas. El motivo se debe a que estas políticas de seguridad deben cumplirse globalmente, de hay la dificultad que entraña el llevar a cabo un despliegue que resulte eficiente. De echo, algunas opiniones apuntan a que NAC puede considerarse como el nuevo IDS (Intrusion Detection System, sistema de detección de intrusos), con la diferencia que la primera de estas tecnologías se despliega de la manera más abierta posible a fin de reducir su impacto en el acceso a la red, resultando más efectivas.

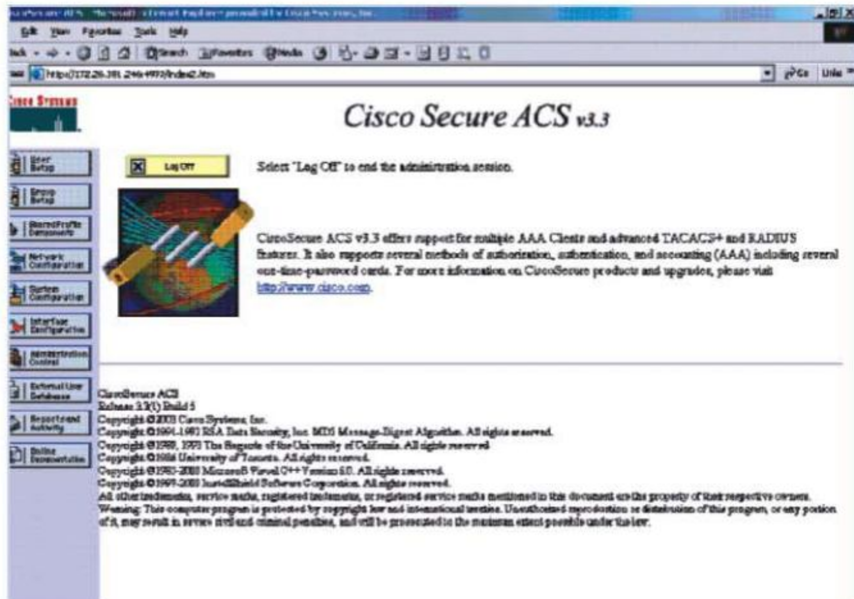
Por lo general, estas políticas se suelen cumplir, aunque el problema está en que, en muchos casos, el malware se adentra en los sistemas a causa de una cierta colaboración inconsciente, es decir, que el usuario no tiene el conocimiento necesario para saber que con determinadas acciones está abriendo la puerta precisamente a dichas amenazas. Esta situación, por lo tanto, exige que el usuario conozca las políticas de seguridad implantadas a este respecto. De esta manera, por ejemplo, estarían en condiciones de identificar un correo phising (o de suplantación de identidad) y contribuir a evitar un ataque o una infección, salvaguardando los datos confidenciales.

Perspectivas de futuro

Todo parece indicar que la evolución de la tecnología NAC viene marcada por el ritmo







Pantalla de bienvenida a Cisco Secure ACS

de la sociedad. En estos instantes, se está apostando fuertemente por la movilidad y el teletrabajo con el siguiente propósito: maximizar el rendimiento de los usuarios, una situación que obliga a dotarse de nuevos mecanismos que garanticen una conexión y autenticación segura y que permita tener la confianza certera de que su red está protegida de principio a fin. Hay que valorar, de igual modo, que los delincuentes sobre todo buscan pasar desapercibidos, un hecho que obliga a extremar las precauciones todavía más.

En otro orden de cosas, la seguridad del punto final resulta uno de los temas más "calientes" actualmente en esta área de negocio. Ya no importa únicamente cómo se define el perímetro, sino todos los dispositivos susceptibles de ser conectados. Así, y en la medida en que se incrementa su número, mayor es la posibilidad de introducir problemas en la red, motivo por el cual la tecnología NAC adquiere una importancia esencial. El futuro pasa, a este respecto, por apostar por una perspectiva lo más amplia posible ya que las redes son cada vez más complejas y abiertas, y porque los dispositivos IP que pueden engancharse a la red no dejan de aumentar. Asimismo, la tecnología NAS dirige sus pasos hacia soluciones convergentes que puedan gestionar por ellas solas el acceso a la red ya que las tareas de control no se limitan de manera única al usuario, sino que atañen a otros factores también importantes como la integridad de los equipos al conectarse a la red.

>>> AMENAZAS DE SEGURIDAD COMBATIDAS

- **Acceso no autorizado a redes LAN, VPN y WLAN**
- **NAS exige que el usuario mantenga actualizado sus parches y firmas de seguridad antes de poder acceder. De lo contrario, no puede hacer nada para detener el ataque que se dirija a un equipo al que la entrada se le ha autorizado.**
- **Esta tecnología ayuda a combatir un gran número de códigos maliciosos como spyware, troyanos, robos de identidad y gusanos, además de intrusiones en el host, accesos.**
- **Posibilidad de verificar la integridad de los accesos realizados a la red por parte de los usuarios.**
- **Tener el control de los usuarios que acceden a una red.**





Regresa el simulador de fútbol por excelencia

Si existe una franquicia de fútbol superventas ésa es, sin lugar a dudas, la de FIFA. Su nueva versión viene cargada de muchas novedades, aunque existe una que destaca sobre el resto: nos referimos a su jugabilidad. Y es que las mejoras en la capacidad de respuesta de los jugadores y la inteligencia artificial en la que sus desarrolladores han trabajado permiten disfrutar de un increíble grado de realismo; tanto es así que una vez que los deportistas aparecen en el terreno, la sensación es la de estar en un partido de los de verdad. El ritmo de las jugadas o el ambiente de las gradas es un buen ejemplo de ello. Aunque, eso sí, antes de pisar el césped hay que trabajar a fondo la técnica individual a través del "modo entrenamiento" para lograr la mejor preparación física. Otro modo que resulta interesante es el "manager": en esta nueva versión, se han introducido hasta medio centenar de mejoras. Esto permite que los resultados de los encuentros se basen en las fortalezas (pero también debilidades) de los jugadores y sus equipos, o que en el mercado de los traspaso se tenga en cuenta, por ejemplo, el prestigio de cada uno de ellos.

En el campo

El sistema de control del balón es mucho más avanzado, tanto que ahora los jugadores son más conscientes de cual es su posición más cómoda y natural para hacerse con el esférico y controlarlo de la forma más sencilla posible. Así, si los jugadores inician una jugada de ataque no sólo se limitan a correr: también analizan el terreno de juego con mayor eficacia, intentado abrirse paso en el césped con una gran variedad de opciones de ataque (por ejemplo, inventando líneas de pases). Por otro lado, la defensa de los equipos tiene la habilidad de desplegar varias jugadas simultáneamente gracias a su mayor inteligencia. Esto se conoce con el nombre de posicionamiento avanzado.

Especialmente interesante es su sistema de regate de 360º, gracias al cual ese mayor control del balón (al que antes nos hemos referido) posibilita que el futbolista encuentre espacios entre la defensa, una situación que antes no se daba. Tampoco defrauda el concepto de "Libertad de juego físico" con un sistema de lucha cuerpo a cuerpo y un regate más amplio con un simple toque al esférico. Precisamente, y si lo tuyo son los rega-



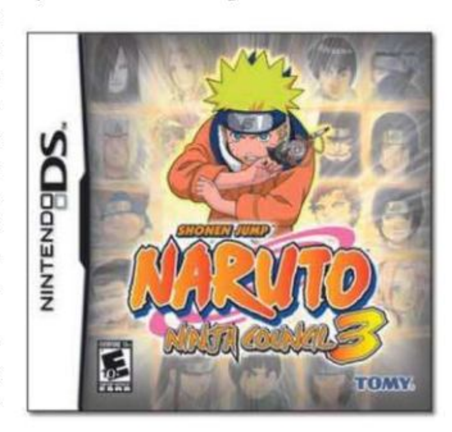
tes, disfrutarás de la novedosa tecnología de sincronización de animación con un control sin precedentes. ¿Te imaginas realizar un magistral regate lateral tan preciso que seas capaz de superar en velocidad y movimiento al blaugrana Piqué?

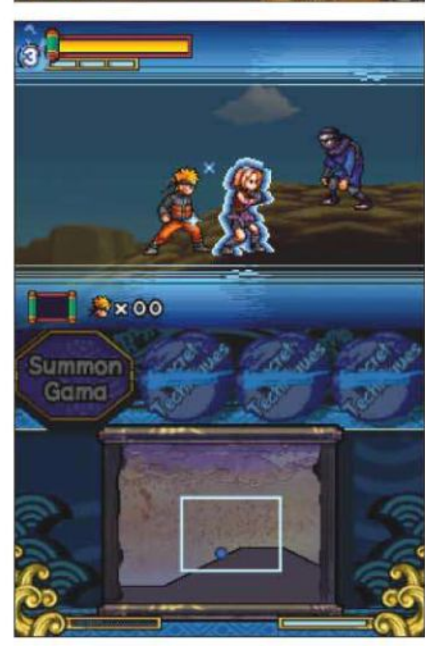
Pero este nuevo FIFA además promete mayor diversidad de disparos realistas, y una mejora de las entradas y la lógica de los despejes para que la línea de la defensa disponga de más opciones y, de esta manera, llegar antes que el contrario a la pelota. Las entradas a ras de suelo y los despejes de chilena tampoco defraudan. Los porteros ahora también se anticipan antes a las jugadas con una mayor precisión. Su percepción ha mejorado con creces a la hora, por ejemplo, de interceptar los balones perdidos.

Anímate a proteger los poderes chakra del ninja adolescente

El videojuego perfecto para los amantes del anime y, en especial, de las aventuras de Naruto. Cuando los poderes chakra del ninja y los de sus amigos se vean amenazados por la malvada organización Akatsuki, serás el encargado de intentar protegerlos y evitar que se hagan con ellos. En la piel de Naruto, Sakura, Neji, Rock Lee o Kakashi tendrás que enfrentarte a sus enemigos en distintos niveles de desplazamiento lateral. La mayoría de estas pantallas permiten escoger dos personajes de apoyo que presten ayuda durante la lucha y, además, elegir con cuál de ellos jugar mientras dura el combate con sólo tocar la pantalla táctil de tu Nintendo DS. Esta superficie también funciona a modo de mapa durante las pausas en el juego, ofreciendo una vista aérea del entorno que ayuda a planificar el camino a seguir, y permite seleccionar los movimientos característicos de cada personaje.

Durante la partida aparecen distintos minijuegos. Cada vez que resuelvas uno podrás activar ataques y conseguir nuevos movimientos para los ninjas. Incluso desbloquear movimientos y luchadores según avanza la partida. Además, es importante tener en cuenta que los poderes chakra disminuirán cada vez que se utiliza un movimiento ninja, así que no se pueden desperdiciar. El título también permite jugar en una red local de entre 2 y 4 jugadores. Además, en la lucha on line, a través de Wi-Fi, es fácil retar a tus amigos: sólo tienes que intercambiar códigos.







MARVEL ULTIMATE ALLIANCE 2





Los superhéroes se enfrentan en una Guerra Civil para proteger su identidad

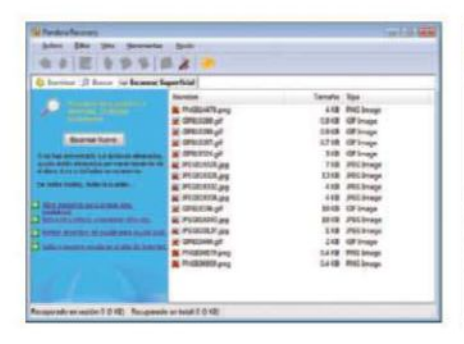
Después del duro enfrentamiento del Doctor Muerte y su ejército de villanos contra Nick Furia y los superhéroes, la población se ha vuelto contra ellos. Por eso, ha aparecido una Ley de Registro mediante la que las personas con poderes tienen que estar inscritos y descubrir sus identidades ocultas. Los superhéroes se han dividido en dos bandos enfrentados y se ha desatado una Guerra Civil: el grupo liderado por Iron Man está a favor de la ley y, contra ellos, el Capitán América y los suyos. Como jugador, debes elegir uno de los dos y luchar con su ejército, utilizando las fuerzas de cuatro superhéroes. Incluso es posible unir sus superpoderes para desatar nuevos ataques, como por ejemplo, un tornado de fuego gracias a Tormenta y Antorcha Humana. En total, con estas combinaciones se pueden crear hasta 250 nuevas fusiones.

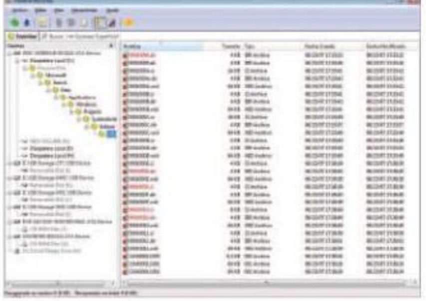
Otra opción interesante es la personalización de los superhéroes: actualizar sus habilidades según avanza el juego y modificar algunas opciones para influir en su carácter. La experiencia de juego es cinemática y con entornos inmersivos, y cada jugador puede interactuar con el entorno de la manera que considere oportuna en cada caso, destruyéndolo a su paso o utilizándolo para conseguir sus fines. A Marvel: Ultimate Alliance 2 se juega de manera individual, pero también con otros jugadores formando equipos de hasta 24 personajes que lucharán juntos o en bandos opuestos para intentarar erigirse vencedores en la guerra.





Recuperar los datos borrados por error





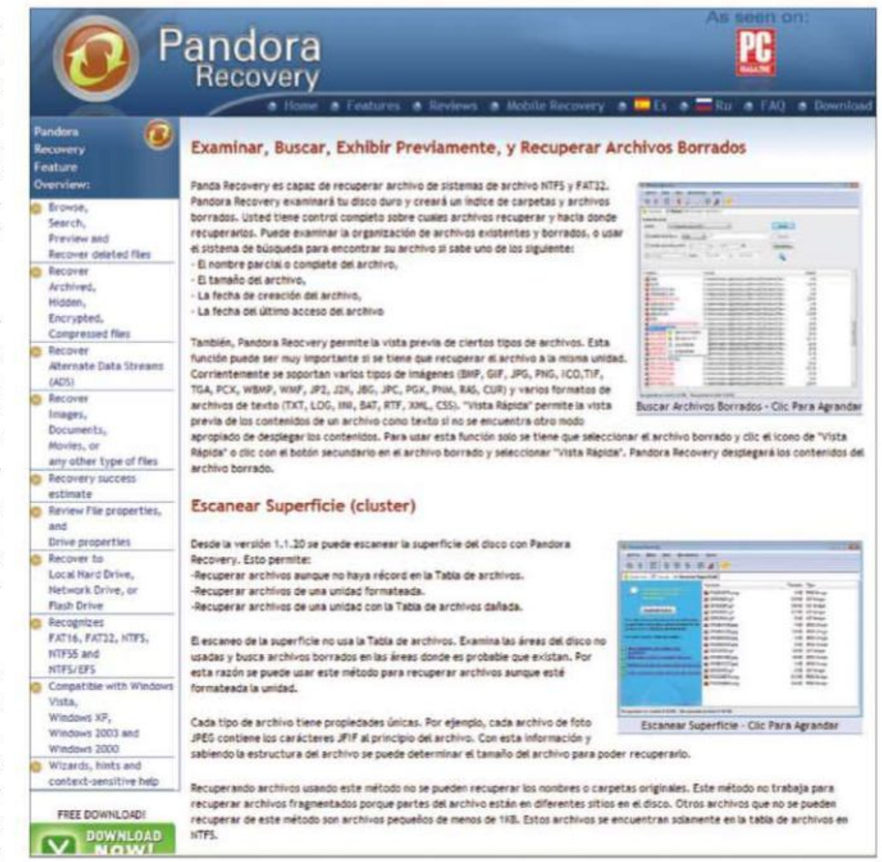


¿Cuántas veces has borrado un documento que hay que entregar una semana después en el trabajo? ¿O esa foto que estaba en el escritorio y a la que tenías tanto cariño?

El programa Pandora Recovery (descargable en la web **www.pandorarecovery.com**) hará posible recuperar archivos eliminados que no se encuentren en la papelera de reciclaje. Una vez se instala la aplicación y se abre, se debe ir a la pestaña de Examinar y seleccionar la capeta o unidad en la que se desean buscar los archivos eliminados.

La búsqueda comenzará de manera automática. Tras localizarlos, los clasifica por colores: en rojo los sobrescritos y, en teoría, no recuperables; en negro los no sobrescritos y recuperables; en azul los comprimidos y en verde los que se encuentran codificados criptográficamente. Es posible tener una vista preliminar del archivo antes de recuperarlo marcando la opción Vista/Mostrar ventana de manera previa.

Para recuperarlo, se pincha en el botón derecho sobre el documento y se selecciona la opción 'Recuperar en'. Surge una ventana donde navegar hasta el lugar del disco en el que se va a dejar el fichero. Se localiza y se pulsa entonces en 'Recuperar Ahora'. Es posible buscar archivos eliminados haciendo uso de las dos pestañas restantes: 'Buscar' o 'Escanear superficie'. Esta última es la más efectiva pero tarda bastante tiempo, incluso horas, por lo que sólo es recomendable utilizarla cuando con la opción 'Examinar' no se encuentra lo que se necesita.





¿Cómo saber cuando se tiene un troyano?

Los troyanos no son precisamente virus que destaquen por pasar inadvertidos, más bien haceN ejecutar al PC una serie de operaciones automáticas propias de una película de ciencia ficción. Aquí enumeramos cuáles pueden ser algunos de los síntomas de su presencia en un sistema:

- Archivos aparecen y desaparecen
- Se ralentiza todo el sistema
- Se bloquea y reinicia el sistema continuamente sin que exista un motivo específico
- Aparecen archivos temporales sin ningún motivo
- Se inician o finalizan programas sin justificación
- El teclado deja de funcionar
- La bandeja del CD se abre y cierra sin que se le ordene
- El servidor de Internet no reconoce nuestro nombre y contraseña o indica que ya está siendo utilizado. Lo mismo sucede con el correo.
- Salen sonidos inexplicables por sus altavoces
- Presencia de ficheros TXT o sin extensión en el HD (normalmente en -c:-) en los que se reconocen palabras/frases/conversaciones/comandos... que han sido escritos anteriormente
- Se avisa de una actividad en el módem cuando no se está realizando ninguna comunicación
- Presencia de archivos y/o carpetas con caracteres extraños
- Aparición de una ventana con un mensaje del tipo: "Te he metido un troyano"



Ejemplo de un troyano que se propaga a través del Messenger

¿Funciona correctamente tu antivirus?

Hasta que, en 1996, el Instituto Europeo para la Investigación de los Antivirus Informáticos (EICAR) desarrollase un test para que los usuarios chequeasen la efectividad de sus sistemas de protección, éstos se veían forzados a usar un malware real para asegurarse de que realmente gozaban de una óptima protección. En la actualidad, todos los primeros fabricantes de antivirus del mundo dan soporte al test de EICAR. Por ello, puede ser interesante hacer la prueba de manera sencilla.

En primer lugar, se descarga el archivo-test en la web **http://www.eicar.org/anti_virus_test_file.htm** y se le coloca una extensión .com, de este modo se asegura de que el programa antivirus que está instalado va a escanear el archivo. Posteriormente se guarda en el disco duro del PC y se inicia el antivirus. Si no lo detecta, es posible que sea necesaria una actualización (a no ser de que se trate de una incompatibilidad con el archivo de test EICAR). Después de que se haya llevado a cabo la comprobación, se prescinde del archivo. Ahora el usuario verá cómo tiene lugar la actualización del sistema o, en caso contrario, se deberá instalar un nuevo sistema de seguridad que tenga una mayor eficacia. Es importante asegurarse también de que se suprime el archivo del disco duro para que no provoque alarmas cada vez que se active la solución del antivirus.



Zona móviles

LOONEYTUNES MONSTER MATCH

Te propone el clásico tres en raya, pero con el aliciente de jugar con tu Looney Tunes favorito: el Pato Lucas, Tweety o Bugs Bunny, entre otros. Una vez que has elegido el que más te gusta lucharás contra los enemigos chiflados que aparecen en tu camino con el objetivo de salvar a la ciudad Acme del ataque del malvado doctor Fricktenstein. Para ello, lo que tienes que hacer es alinear 3 o más fichas y derrotar a su ejército. El título tiene una estética muy colorista y llena de vida. A media que la partida se desarrolla, descubres animaciones únicas que reflejan a la perfección la personalidad de cada uno de estos entrañables personajes. Además, existe la posibilidad de revivir legendarias rivalidades como la de Tweety contra Silvestre. ¿Te apuntas?

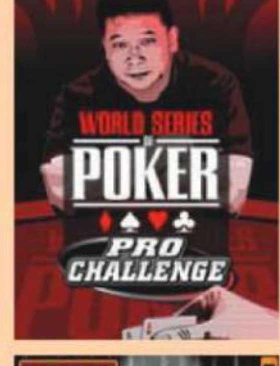






WORLD SERIES OF POKER PRO CHALLENGE

Los aficionados al póker, uno de los juegos de cartas más emocionantes que existen, están de enhorabuena. De la mano de Glu Mobile, y a través de la tienda de Windows Marketplace Mobile, tienen la oportunidad de hacerse con World Series of Poker Pro Challenge y enfrentarse a algunas de las grandes celebridades de este juego como Chris Ferguson, Johnny Chan, Scotty Nguyen o Shannon Elisabeth, entre otros profesionales. Se trata de una oportunidad única e irrepetible que seguro que no estás dispuesto a dejar pasar. Lo interesante es que no sólo te limitas a jugar tus cartas correcta (y magistralmente) para conseguir el reconocimiento de tus adversarios, sino que también puedes estudiar sus reacciones y adelantarte a ellas a medida que la partida transcurre. ¿Serás capaz de echarte un auténtico farol o tal vez la presión pueda contigo y decidas que lo mejor es saber retirarte a tiempo?









MINI GOLF CHIHUACA



En escenarios tan originales como una isla volcánica, una nube o las cimas de "Luna de Queso", Mini Golf Chihuaca te invita a conocer un campo de golf diferente y, sobre todo, divertido. En total, descubrirás hasta cuatro campos temáticos con nueve hoyos: País de Tiki o Polo Norte son sólo dos de ellos. Para los jugadores más clásicos, se incluye el modo de juego "Golpear". Aunque si eres de los que siempre va con el tiempo justo, tu modalidad es la "Contra Reloj". En último lugar, te echarás unas cuantas risas con el modo "Ardilla Golf" evitando a las ardillas y a sus trampas diabólicas. Con escenarios interactivos y gráficos en 3D, tienes la opción de descargarte nuevos componentes y personalizar a los personajes. Puedes conseguir suculentas recompensas y desbloquear campos ganando puntos. El titulo está disponible sólo para el iPhone.



